SISTEMA PENALE

FASCICOLO
4/2020

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

ISSN 2704-8098

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervè Belluta, Michele Caianiello, Massimo Ceresa-Gastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Risicato, Marco Scoletta, Carlo Sotis, Costantino Visconti

COMITATO SCIENTIFICO Alberto Alessandri, Silvia Allegrezza, Ennio Amodio, Gastone Andreazza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Fabio Basile, Alessandra Bassi, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Rocco Blaiotta, Manfredi Bontempelli, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Carlo Fiorio, Roberto Flor, Luigi Foffani, Désirée Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kostoris, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Grazia Mannozzi, Marco Mantovani, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocolo, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Andrea Francesco Tripodi, Giulio Ubertis, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vigoni, Francesco Zacchè, Stefano Zirulia

REDAZIONE Francesco Lazzeri (coordinatore), Alberto Aimi, Enrico Andolfatto, Enrico Basile, Silvia Bernardi, Carlo Bray, Pietro Chiaraviglio, Stefano Finocchiaro, Beatrice Fragasso, Alessandra Galluccio, Cecilia Pagella, Tommaso Trinchera, Maria Chiara Ubiali

Sistema penale (*SP*) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.
La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.
La *Rivista* si uniforma agli standard internazionali definiti dal *Committe on Publication Ethics* (COPE) e fa proprie le relative linee guida.

I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili).
Il testo completo della licenza è consultabile su *https://creativecommons.org/licenses/by-nc-nd/4.0/*.

Peer review I contributi che la direzione ritiene di destinare alla sezione "*Articoli*" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezo "*Altri contributi*" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.
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 *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen.* (o *SP*), 1/2020, p. 5 ss.

4/2020

PRESUPPOSTI E LIMITI ALL'UTILIZZO DEL CAPTATORE INFORMATICO: LE INDICAZIONI DELLA SUPREMA CORTE (*)

di Luigi Giordano

Nel contributo che segue viene compiuta una completa panoramica sulla giurisprudenza di legittimità sul tema dei presupposti e dei limiti all'utilizzo del captatore informatico per effettuare intercettazioni. È l'occasione per soffermarsi anche su delicate questioni di diritto intertemporale, concernenti in particolare l'utilizzo dei risultati di tali captazioni come prova dei reati contro la pubblica amministrazione in attesa dell'efficacia delle disposizioni di cui al d.lgs. n. 216 del 2019 come modificate dal d.l. n. 161 del 2019, convertito con modifiche dalla legge n. 7 del 2020.

(*) Il contributo costituisce una versione rivista della relazione svolta dall'autore in data 11 febbraio 2020 in occasione del Corso "*Disciplina e tecnica di effettuazione delle intercettazioni di comunicazioni interpersonali alla luce delle novità normative e del diritto vivente*", organizzato dalla Scuola Superiore della Magistratura, a Napoli – Castelcapuano.

1. La sentenza "Scurato": l'uso del captatore informatico nei soli procedimenti per delitti di criminalità organizzata.

L'esame delle indicazioni della giurisprudenza di legittimità sul tema dei presupposti e dei limiti all'impiego del "captatore informatico" nelle indagini deve necessariamente partire dalla sentenza delle Sezioni unite del 28 aprile 2016, n. 26889, Scurato[1]. Con questa decisione, come è noto, la Corte, in considerazione della natura itinerante dei dispositivi adoperati come moderne microspie – *smartphone*, *tablet*, computer – e del fatto che tali dispositivi accompagnano le persone anche nelle abitazioni e nei luoghi più intimi delle stesse, ha affermato che il nuovo strumento è utilizzabile per realizzare intercettazioni "tra presenti" nei soli procedimenti per delitti di criminalità organizzata. In questi casi, infatti, trova applicazione la disciplina di cui all'art. 13 del decreto legge n. 151 del 1991, convertito dalla legge n. 203 del 1991, che, derogando ai presupposti fissati dall'art. 266, comma 2, cod. proc. pen., permette la captazione anche nei luoghi di privata dimora, senza che sia necessario che tali luoghi siano sedi di attività criminosa in atto. Al contrario, l'utilizzo del nuovo mezzo tecnologico è stato escluso per i reati comuni perché, non essendo possibile prevedere i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, nel momento dell'autorizzazione, non sarebbe possibile verificare il rispetto della condizione di legittimità richiesta dall'art. 266, comma 2, cod. proc. pen. che presuppone, per la legittimità delle captazioni in luoghi domiciliari, che sia in atto l'attività criminosa[2].

---

* Il contributo costituisce una versione rivista della relazione svolta dall'autore in data 11 febbraio 2020 in occasione del Corso "*Disciplina e tecnica di effettuazione delle intercettazioni di comunicazioni interpersonali alla luce delle novità normative e del diritto vivente*", organizzato dalla Scuola Superiore della Magistratura, a Napoli – Castelcapuano.

[1] Cass., Sez. un. 28 aprile 2016, n. 26889 (dep. 1 luglio 2016), Scurato, in *Arch. nuova proc. pen*. 2017, 76 e ss. con nota di A. CAMON, *Cavalli di troia in Cassazione*; in *Cass. pen*. 2016, 2274-2288, con nota di A. BALSAMO, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*; in *Il Diritto dell'informazione e dell'informatica*, 2016, 88, con nota di G. CORASANITI, *Le intercettazioni "ubiquitarie" e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*; in *Proc. pen. giust*., 2016, 5, 21, con nota di P. FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*. Sulla sentenza si veda anche A. GAITO, S. FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen*. 2016, 2, 309; A. CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite*, in *Arch. pen*. 2016, 2, 331; L. FILIPPI, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia (a proposito del captatore informatico)*, in *Arch. pen*. 2016, II, 348; L. PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen*. 2016, II, 354; G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, cit.; F. CAPRIOLI, *O "captador informático" como instrumento de busca da prova na Itália*, in *Revista Brasileira de Direito Processual Penal*, 2017, 484 e ss.; più di recente, P. BRONZO, *Intercettazione ambientale tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 235 e ss. Sulla sentenza, sia consentito il rinvio anche a L. GIORDANO, *Dopo le Sezioni unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont*. 2017, 3, 184 e ss.

[2] L'apertura del sistema delle indagini penali in Italia a forme di intercettazioni effettuate tramite captatori

Questa sentenza, come è pure noto, ha suscitato un dibattito particolarmente animato, nell'ambito del quale si sono manifestate posizioni nettamente contrapposte[3]. In particolare, sono state espresse obiezioni all'esclusione dell'uso del *malware* per le indagini relative a reati diversi da quelli di criminalità organizzata.

È stato ipotizzato, infatti, che l'autorizzazione ex art. 267 cod. proc. pen. del giudice perle indagini preliminari potrebbe essere circoscritta alle conversazioni che avverranno in un luogo pubblico o aperto al pubblico. Questa condizione, evidentemente, permetterebbe il rispetto del limite allo svolgimento di intercettazioni di dialoghi tra presenti in ambienti domiciliari di cui all'art. 266, comma 2,cod. proc. pen.

---

informatici rappresenta un passo necessario nell'attuale contesto storico. In questo termini, tra gli altri, G. LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *Dir. pen. contemp.*, 7 ottobre 2016, 22. Il *trojan*, ad esempio, è considerato uno strumento d'indagine «imprescindibile» per superare la difficoltà di intercettare le comunicazioni VOIP – acronimo di *Voice Over Internet Protocol* – ed i flussi di comunicazioni gestite da Internet service provider americani come *Microsoft*, *Google*, *Yahoo* ed *Apple* come ha precisato F. CAJANI, *Odissea del captatore informatico*, in *Cass. pen*. 2016, 4143; più di recente, F. CAJANI, *Le indagini informatiche per i reati di Cyberterrorismo*, in Cadoppi, Canestrari, Manna (a cura di), *Cybercrime*, Milano, 2019, 1540 e ss.. Su questo aspetto del tema sia consentito il rinvio anche a L. GIORDANO, *La disciplina del captatore informatico*, in T. Bene (a cura di), *L'intercettazione di comunicazioni*, Bari, 2018, 266. In dottrina è stata coniata l'espressione "metamorfosi investigativa" per designare l'apertura all'impiego degli strumenti informatici nelle indagini (S. SIGNORATO, *Le indagini digitali; profili strutturali di una metamorfosi investigativa*, Torino, 2018, 1; G. DI PAOLO, *Tecnologie del controllo e prova penale. L'esperienza statunitense e spunti per la comparazione*, Padova, 2018, *passim*).

[3] Un orientamento ha espresso critiche decise, che sono state compendiate finanche in una "*Denuncia dei rischi connessi all'installazione occulta di virus informatici su smartphone e tablet per finalità di indagine penale*", diffusa nel luglio 2016 da alcuni docenti universitari, con la quale, traendo spunto dalla preoccupazione ingenerata dal fatto che le Sezioni unite avevano affermato la legittimità, sia pure a determinate condizioni, dello strumento in esame per compiere intercettazioni, si è auspicato l'intervento del legislatore per regolare la materia al fine di realizzare un adeguato bilanciamento dei principi costituzionali e convenzionali coinvolti (La denuncia è reperibile in rete nel sito istituzionale dell'Università di Torino). Una diversa opinione (R. ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen. (web)*, 25 luglio 2016), invece, ha invitato a distinguere l'uso della moderna tecnologia informatica per effettuare intercettazioni tra presenti – che trova nelle disposizioni dapprima citate la fonte "base normativa" – dal suo impiego per svolgere altre attività di ricerca della prova, come perquisire a distanza gli archivi di computer, *tablet*, *smartphone*. Sotto quest'ultimo aspetto è stato affermato che l'impiego del nuovo strumento esulerebbe dal raggio d'azione degli art. 14 e 15 Cost. e, dunque, non basterebbe l'introduzione di una specifica disciplina normativa, ma sarebbe necessario l'affermazione di un nuovo diritto fondamentale all'uso libero e riservato delle tecnologie informatiche, sul modello di quanto avvenuto in altri ordinamenti ed in particolare in Germania, a partire da una nota sentenza Bundesverfassungsgericht 27 febbraio 2008,in *Riv. trim. dir. pen. econ*., 3, 2009, 679 e ss., con nota di FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*., con la quale è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, ed è stato inaugurato un nuovo diritto costituzionale riconducibile alla c.d. "autodeterminazione informativa" e "sicurezza informatica", quest'ultima da intendersi anche come integrità e riservatezza dei dati e delle informazioni trattate da sistemi informatici, fondato sulla dignità umana dell'individuo e dell'utente "informatico". Nel 2016 è intervenuta un'altra pronuncia (Bundersverfassungsgericht, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09, in *Dir. pen. cont.*, 8 maggio 2016, con nota di L. GIORDANO, A. VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*.

Il dispositivo infettato, inoltre, potrebbe essere un personal computer fisso o "non trasportabile", installato in un determinato posto diverso da quelli presi in considerazione dall'art. 614 cod. pen. ovvero in un computer portatile abitualmente tenuto fermo in un luogo pubblico[4]; dunque, anche in questo caso non si porrebbe il problema di garantire la tutela dell'inviolabilità del domicilio.

Più in generale, è stato evidenziato che l'agente intrusore con cui è infettato il dispositivo elettronico è controllabile a distanza; il "microfono" può essere acceso o spento a richiesta; lo *smartphone* può essere "tracciato"; in questo modo potrebbe essere evitato di procedere a registrazioni quando il portatore del telefono infettato con il programma *trojan* entra in un domicilio[5].

Queste critiche , chiaramente, sono state rivolte ad evidenziare i limiti strutturali della decisione delle Sezioni unite, il cui vizio di fondo consisterebbe nel mancato approfondimento delle potenzialità tecniche-operative del nuovo strumento[6].

2. segue: La scelta di fondo delle Sezioni unite.

I rilievi illustrati, che, come meglio si vedrà nel prosieguo, hanno inciso su talune soluzioni offerte dalla giurisprudenza di merito alle questioni emerse, permettono di cogliere la scelta più profonda operata dalla sentenza "Scurato".

In considerazione della profonda invasività del mezzo tecnologico in esame e dei connessi rischi per la libertà di comunicare anche degli eventuali terzi che entrano in contatto con il detentore del dispositivo "infettato", le Sezioni unite non hanno voluto legittimare l'adozione di un'autorizzazione di intercettazioni "al buio", cioè concessa dal giudice senza poter valutare preventivamente lo svolgimento di attività criminosa nel luogo domiciliare in cui potrebbe essere introdotto il dispositivo, ritenuto non prevedibile[7]. La Corte, dunque, ha inteso evitare alla radice il rischio di intercettazioni tra presenti in luoghi di privata dimora, anche "oltre le intenzioni" accolte dal provvedimento autorizzativo.

In verità, sarebbe stato possibile adottare soluzioni diverse.

---

[4] L'esempio è tratto da G. AMATO, *Reati di criminalità organizzata: possibile intercettare conversazioni o comunicazioni con un captatore informatico*, in *Guida al dir*. 2016, n. 34-35, 79.

[5] E. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle sezioni unite*, in *Parola alla difesa*, 2016, 1, 161.

[6] È stata proposta, in verità, una lettura della sentenza delle Sezioni unite secondo cui essa, nei procedimenti relativi a reati diversi da quelli di criminalità organizzata, legittimerebbe l'uso del *trojan* sia nei luoghi che rientrano nella previsione dell'art. 614 cod. pen. preventivamente indicati nella richiesta di autorizzazione, se ivi si sta svolgendo l'attività criminale, sia in luoghi di natura non domiciliare comunque specificamente individuati. Si afferma che, in entrambi i casi, sono rispettati i principi di garanzia, perché non si correrebbe il rischio di realizzare intercettazioni tra presenti in luoghi di privata dimora e l'autorizzazione sarebbe concessa sulla base di adeguati controlli (F. CAJANI, *Odissea del captatore informatico*, cit., 4149).

[7] Nella sentenza, sul punto, è precisato: «Se anche fosse tecnicamente 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 nel momento dell'autorizzazione ….».

Per esempio, poteva essere ritenuta sufficiente a garantire le prerogative individuali di cui all'art. 2 e 14 Cost. la dichiarazione di inutilizzabilità ex art. 271 cod. proc. pen. delle eventuali registrazioni che fossero state compiute in un domicilio, per reati comuni e senza che fosse in corso l'attività criminosa – dunque, "*fuori dei casi consentiti dalla legge*" o fuori dai limiti dell'autorizzazione – applicando un meccanismo di tutela già adoperato in tema di intercettazioni[8].

Le Sezioni unite, tuttavia, hanno reputato insoddisfacente la garanzia "postuma" dei diritti individuali che deriverebbe dall'applicazione della sanzione processuale appena indicata: l'inutilizzabilità, secondo la Corte, va invece riservata a gravi patologie degli atti del procedimento e non all'ipotesi di adozione di provvedimenti *contra legem* e non preventivamente controllabili quanto alla loro conformità alla legge.

Nella sentenza "Scurato", inoltre, le Sezioni unite hanno manifestato la consapevolezza che il nuovo strumento investigativo possa prestarsi a strumentalizzazioni, nel senso che possa essere impiegato al di fuori dei casi di indagini relative a reati di "criminalità organizzata".

Riconoscendo la particolare forza intrusiva del mezzo sulle prerogative individuali, infatti, la Corte ha precisato che «la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso».

A queste affermazione è sotteso una sorta di invito a valorizzare (o, forse, a recuperare) la funzione di garanzia del decreto che autorizza le intercettazioni.

L'impiego del mezzo tecnologico, in altri termini, non muta il problema principale della disciplina delle intercettazioni. Il bilanciamento tra i diritti costituzionali individuali e collettivi in conflitto deve intervenire nella motivazione del provvedimento autorizzativo[9].

Di recente, affrontando un altro tema, le Sezioni unite della Corte di cassazione hanno affermato che «L'autorizzazione del giudice non si limita a legittimare il ricorso al mezzo di ricerca della prova, ma circoscrive l'utilizzazione dei suoi risultati ai fatti-reato che all'autorizzazione stessa risultino riconducibili»[10].

---

[8] Si pensi al divieto di intercettazione dei colloqui tra il difensore e l'indagato di cui all'art. 103, comma 5, cod. proc. pen. che, secondo l'indirizzo consolidato della Corte di cassazione, non sussiste quando le conversazioni o le comunicazioni intercettate non siano pertinenti all'attività professionale svolta dalle persone indicate nell'art. 200 cod. proc. pen. e non riguardino di conseguenza fatti conosciuti per ragione della professione dalle stesse esercitata, sicché l'utilizzabilità valutata dopo la registrazione dei dialoghi (cfr., di recente, Cass., Sez. 4, n. 55253 del 05/10/2016, in *CED Cass.* n. 268618 Cass., Sez. 6, 17 marzo 2015, n. 18638 (dep. 5 maggio 2015), in *CED Cassazione* n. 263548; Cass., Sez. V, 25 settembre 2014, n. 42854 (dep. 13 ottobre 2014), in *CED Cassazione* n. 261081).

[9] Secondo Cass. pen, Sez. 6, 20 ottobre 2009 (dep. 31 dicembre 2009) n. 50072, in *Giur. It.* 2010, 12, 2649, «la imprescindibile funzione del giudice, cui è demandato lo scrutinio dei presupposti di attivabilità delle intercettazioni, è quella di affermare in ogni momento il rispetto della legalità del procedimento e non certo quella di prestarsi a "facili aggiramenti" delle norme di legge per compiacere alle richieste del pubblico ministero o di chicchessia».

[10] Cass., Sez. U, 28 novembre 2019, dep. 2020, n. 51, Cavallo ed altro, in *CED Cass.* n. 277395.

Pur dovendo essere sobria e, dunque, potendo consistere in quella «minima necessaria a chiarire le ragioni del provvedimento»[11], la motivazione del decreto autorizzativo deve spiegare che il mezzo di ricerca della prova «è assolutamente indispensabile ai fini della prosecuzione delle indagini» rispetto ad una determinata, specifica e seria ipotesi delittuosa[12].

Come ha indicato da tempo la Suprema Corte[13], il giudice deve dare conto della ragione della compressione della libertà di comunicare di una determinata persona, illustrando quale sia il suo rapporto con le specifiche investigazioni in atto. Per giustificare l'atto investigativo, in altri termini, il giudice non può tralasciare di indicare il criterio di collegamento tra l'indagine in corso e l'intercettando (che, come è noto, ben può essere una persona non sottoposta ad indagine).

3. I riflessi della sentenza "Scurato" nella giurisprudenza successiva.

Dopo l'intervento delle sezioni unite, il tema dell'utilizzabilità dei risultati delle intercettazioni compiute tramite *trojan* è stato affrontato da diverse decisioni della Corte di Cassazione, il cui numero, peraltro, appare limitato. Questo dato non è neutro, perché le peculiarità dello strumento tecnologico usato per le intercettazioni sono tali da

---

[11] Cfr., tra le altre, Cass. pen., Sez. 5, 20 aprile 2004, n. 24229, in *Guida al diritto* 2004, 26, 76, secondo cui è sufficiente che il giudice indichi i dati da lui ritenuti decisivi e non è necessario operare uno specifico esame critico dell'intero contesto sottoposto al suo esame. Il giudice, tuttavia, deve compiere autonoma valutazione delle richieste degli organi investigativi e non limitarsi ad espressioni che costituiscano perifrasi del contenuto delle norme che disciplinano l'assunzione del mezzo probatorio (Cass. pen., Sez. 6, 22 dicembre 1998, n. 4057, in *Cass. pen.* 2000, 3353).

[12] Cass. pen., Sez. VI, 26 febbraio 2010, n. 10902, in *CED Cassazione* n. 246688, secondo cui "*il presupposto dei gravi indizi di reato va inteso non in senso probatorio, ossia come valutazione del fondamento dell'accusa, ma come vaglio di particolare serietà delle ipotesi delittuose configurate, le quali non devono risultare meramente ipotetiche, essendo al contrario richiesta una sommaria ricognizione degli elementi dai quali sia dato desumere la seria probabilità dell'avvenuta consumazione di un reato*". In questi termini, tra le altre, Cass. pen., Sez. 2, 1 marzo 2005, n. 10881, in *Guida al diritto* 2005, 16, 82; Cass. pen., Sez. un., 17 novembre 2004, n. 45189, in *Riv. pen.* 2005, 1018). La valutazione della particolare serietà dell'ipotesi delittuosa non implica un'esposizione analitica di tutti gli elementi indiziari (è sufficiente solo una ricognizione sommaria), né impone un vaglio critico di tutti gli elementi, che condurrebbe alla valutazione probatoria del fondamento dell'accusa (Cass. pen., Sez. 6, 7 novembre 2006, n. 42178, in *Arch. nuova proc. pen.* 2007, 5, 669; Cass. pen., Sez. II, 21 aprile 1997 n. 2873, in *CED Cassazione* n. 208757). Il presupposto dei "gravi indizi di reato", dunque, non ha una connotazione "probatoria", in chiave di prognosi di colpevolezza, ed esige un vaglio di particolare serietà delle esigenze investigative. Tali esigenze tuttavia vanno riferite ad uno specifico fatto costituente reato, in modo da circoscrivere l'ambito di possibile incidenza dell'interferenza nelle comunicazioni private altrui (cfr. A. Nappi, *Sull'abuso delle intercettazioni*, in *Cass. pen.* 2009, 471).

[13] Cass. pen., Sez. 6, 12 febbraio 2009, n. 12722, in *Giur. It.* 2010, 5, 1186. La vicenda riguardava la declaratoria di inutilizzabilità per mancanza di motivazione di alcuni decreti di intercettazioni redatti con una motivazione *per relationem* alla richiesta del PM, senza che fosse dato conto delle ragioni per cui erano sottoposte ad intercettazioni conversazioni private. Secondo la dottrina (V. GREVI, *Sul necessario collegamento tra utenze telefoniche e indagini in corso nel decreto autorizzativo delle intercettazioni*, in *Cass. pen.* 2009, 9, 3344), con questa decisione la Corte ha lanciato *"un messaggio di tipo pedagogico agli organi applicatori di fronte al rischio, non soltanto teorico, di una eccessiva disinvoltura nel ricorso allo strumento delle intercettazioni"*.

suscitare, una volta impiegato, necessariamente questioni di utilizzabilità nel corso del procedimento e tale genere di questioni, afferendo ai temi della legittimità, sono di norma comunque riproposte in sede di ricorso per Cassazione.

L'esiguo numero di decisioni dimostra che è stato fatto un uso prudente del captatore informatico nelle indagini. Ciò, per un verso, potrebbe essere dipeso dal fatto che anche i magistrati delle Procure della Repubblica hanno percepito la portata invasiva di un mezzo che, peraltro, presenta un costo elevato, difficilmente sostenibile in un epoca in cui è frequente il richiamo a contenere le spese per le intercettazioni; per altro verso, lo scarso numero di procedimenti in cui sono state poste questioni sull'uso del *trojan* può essere derivato da difficoltà di natura tecnica, che non hanno reso possibile le captazioni.

Per usare lo strumento informatico in esame occorre superare complessi problemi pratici (per esempio, l'eccessivo uso delle batterie dei dispositivi portatili, la necessità di sfuggire agli antivirus e ai firewall). Bisogna valicare i blocchi che i tecnici *hardware* e *software* delle grandi compagnie informatiche hanno impostato sui dispositivi per impedire la modificazione delle impostazioni del sistema. Si devono eseguire, per usare il gergo informatico, processi di *Rooting*, in ambiente *Android*, o *Jailbreak*, per chi usa il sistema *Ios*, perché si deve installare un genere di programma che richiede "permessi da amministratore". Non sempre tali azioni possono essere compiute "da remoto" e, dunque senza accedere materialmente al dispositivo. Non sempre, dunque, le operazioni di intercettazioni danno esiti positivi[14].

4. segue: La sentenza "Romeo" del 2017.

Tra le poche sentenze che si sono occupate della disciplina del captatore informatico si segnala Cass., Sez. 6, 13 giugno 2017, n. 36874, Romeo[15].

Il giudizio concerneva l'impugnazione dell'ordinanza con la quale il Tribunale di Roma, sezione riesame, aveva confermato l'ordinanza applicativa della custodia cautelare in carcere nei confronti di un imprenditore per il reato di corruzione. Per quello che qui interessa, tra i motivi proposti dalla difesa, uno riguardava l'utilizzabilità del *trojan* per svolgere intercettazioni in merito ad un'ipotesi delittuosa che, secondo la prospettazione difensiva, non permetteva il suo impiego e, comunque, all'interno di luoghi di privata dimora e al di là dell'effettivo svolgimento in essi di un'attività delittuosa.

La Corte, ritenendo che il Tribunale non avesse compiuto il necessario controllo sul profilo oggetto della specifica eccezione della difesa, ha annullato con rinvio il provvedimento impugnato.

---

[14] Sui meccanismi di funzionamento del captatore informatico, si veda, tra gli altri, R. BRIGHI, *Funzionamento e potenzialità investigative del malware*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 211 e ss., in particolare il par. 4, intitolato "*Funzionamento*".

[15] Su questa sentenza, sia consentito il rinvio a L. GIORDANO, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Dir. pen. cont.*, 27 settembre 2017.

Al riguardo, ha richiamato i principi delineati dalle Sezioni Unite nella sentenza "Scurato", ritenendo possibile l'uso del *trojan* solo per i reati di criminalità organizzata, dovendo intendersi per tali quelli elencati nell'art. 51, commi *3-bis* e *3-quater*, cod. proc. pen. nonché quelli comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.

In particolare, è stato rimarcato un punto della motivazione delle Sezioni Unite, evidentemente ritenuto fondamentale: «In considerazione della forza intrusiva del mezzo usato, la qualificazione del fatto reato, ricompreso nella nozione di criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso».

Secondo la decisione in commento, l'ordinanza impugnata aveva affermato solo in modo apodittico il collegamento tra la genesi dell'attività d'indagine e l'acquisizione di elementi in merito ad un'ipotizzata infiltrazione camorristica nelle attività dei servizi di pulizia svolti dall'impresa del ricorrente presso un ospedale, sebbene detti elementi fossero decisivi ai fini della valutazione di utilizzabilità delle captazioni. La Corte, pertanto, ha devoluto al Tribunale del riesame nel giudizio di rinvio di verificare, nel materiale indiziario raccolto, la sussistenza di elementi di collegamento della condotta delittuosa oggetto del tema d'accusa cautelare con l'esistenza di associazioni criminali, in quanto solo in questo modo che avrebbe potuto giustificare l'utilizzazione del captatore informatico.

La sentenza, poi, ha aggiunto un secondo accertamento a quello appena descritto, consistente nell'accertamento della «coincidenza tra le ipotesi delittuose oggetto delle iscrizioni effettuate nel registro delle notizie di reato ex art. 335 cod. proc. pen. e quelle poi indicate nelle richieste e nei correlativi decreti di autorizzazione e proroga delle intercettazioni utilizzate nel presente procedimento che si riferiscono alla configurazione dell'ipotesi delittuosa ivi provvisoriamente contestata».

Anche tale accertamento, francamente più discutibile, è evidentemente finalizzato a verificare la sussistenza dei presupposti per l'utilizzazione del cd. *trojan* al fine di compiere intercettazioni ambientali, dal momento che, come è stato più volte evidenziato in precedenza, secondo la sentenza Scurato, in ragione della portata invasiva dello strumento tecnologico, esso deve essere riservato alle indagini relative ai soli reati di criminalità organizzata.

Questo secondo profilo, invero, presenta implicazioni molto delicate, come peraltro rilevato nella stessa sentenza in esame.

Per un verso, infatti, è stato precisato che la legittimità di un'intercettazione deve essere verificata al momento in cui la captazione è richiesta ed autorizzata, «non potendosi procedere ad una sorta di controllo diacronico della sua ritualità sulla base delle risultanze derivanti dal prosieguo delle captazioni e dalle altre acquisizioni», con l'importante conseguenza che «nel caso in cui un'intercettazione di comunicazione sia disposta applicando la disciplina prevista dall'art. 13, comma 1, del decreto legge 13 maggio 1991, n. 152 … con riguardo ad una originaria prospettazione di reati di criminalità organizzata, le relative risultanze possono essere utilizzate anche quando il prosieguo delle indagini impone di qualificare i fatti come non ascrivibili alla suddetta area».

Per altro verso, in considerazione del mezzo tecnologico impiegato, occorre rispettare un onere motivazionale particolarmente intenso ai fini dell'emissione del provvedimento autorizzativo, «poiché la forza intrusiva del mezzo usato ed il potenziale *vulnus* all'esercizio delle libertà costituzionalmente tutelate devono essere prudentemente bilanciati con il rispetto dei canoni di proporzione e ragionevolezza, cosicché la qualificazione, pure provvisoria, del fatto come inquadrabile in un contesto di criminalità organizzata risulti ancorata a sufficienti, sicuri ed obiettivi elementi indiziari …».

Quest'ultima considerazione ha portato la Corte a sviluppare quella che appare l'affermazione più rilevante della decisione in commento. Essa consiste nel rilevare che la possibilità di impiegare mezzi tecnologici particolarmente invasivi conduce a rimarcare la funzione di garanzia della motivazione del decreto autorizzativo delle intercettazioni. «Il bilanciamento tra i diritti costituzionali confliggenti, individuali e collettivi, deve intervenire proprio nella motivazione del provvedimento autorizzativo, che in tal senso viene ad assumere una fondamentale funzione di garanzia, spiegando le ragioni dell'assoluta indispensabilità dell'atto investigativo e indicando con precisione quale sia il criterio di collegamento tra l'indagine in corso e la persona da intercettare».

Il presupposto dei gravi indizi di reato, infatti, non ha una connotazione "probatoria", in chiave di valutazione prognostica della colpevolezza, ma esige un vaglio di particolare serietà delle esigenze investigative, che vanno riferite ad uno specifico fatto costituente reato, in modo da circoscrivere l'ambito di possibile incidenza dell'interferenza nelle altrui comunicazioni private.

In particolare, nel caso di richiesta di captazioni che contempli l'uso del programma del tipo "*trojan horse*", s'impone il rigoroso apprezzamento, già nella fase della richiesta, ma soprattutto in quella della successiva autorizzazione giudiziale, della solidità della qualificazione dell'ipotesi associativa, che non deve essere strumentalizzata al fine di ottenere l'autorizzazione di intercettazioni per mezzo del captatore informatico altrimenti non consentite.

5. segue: la sentenza "Di Guardo ed altri" del 2017.

La Corte di Cassazione, poi, è intervenuta sul tema della motivazione del provvedimento che autorizza l'impiego del captatore informatico nel corso delle indagini anche con la sentenza Cass., Sez. 6, 28/02/2017, n. 15573, Di Guardo ed altri[16].

La decisione è stata emessa nell'ambito di un procedimento per reati contro la pubblica amministrazione nel quale sono state disposte intercettazioni ambientali per mezzo del captatore informatico. I fatti oggetto delle indagini, sia nella richiesta del pubblico ministero di autorizzazione allo svolgimento delle intercettazioni, sia nel provvedimento successivamente emesso dal G.i.p., non erano stati ricondotti all'illecito

[16] Per un esame di questa sentenza, volendo, L. GIORDANO, *Intercettazioni per mezzo di captatore informatico: il tribunale può riqualificare il fatto esposto nel decreto del Gip,* in *Ilpenalista.it*, 15 dicembre 2017.

associativo e, dunque, ad un delitto di criminalità organizzata ex art. 13 del d.l. n. 152 del 1991. Il tribunale del riesame, tuttavia, aveva riqualificato tali fatti, ravvisando gli estremi del reato associativo nei fatti desumibili dal primo decreto autorizzativo, in tal modo giustificando l'impiego del mezzo tecnologico in esame per le captazioni.

Nel ricorso per cassazione avverso l'ordinanza del Tribunale del riesame che aveva confermato il provvedimento applicativo della custodia in carcere nei confronti degli indagati, è stata dedotta l'inutilizzabilità dei risultati delle intercettazioni compiute per mezzo del *trojan* in quanto eseguite senza rispettare i principi indicati dalla sentenza "Scurato", rilevando che l'iscrizione per il reato di cui all'art. 416 cod. pen., che legittimava l'impiego dello strumento tecnologico in esame, era avvenuta solo in epoca successiva all'inizio delle operazioni. In ogni caso, secondo la prospettazione difensiva, non sussistevano i presupposti indiziari di tale fattispecie delittuosa, dovendo pertanto concludersi per l'inutilizzabilità dei risultati delle captazioni.

La Corte, rigettando il ricorso, ha reputato infondato questo motivo, rilevando che il Tribunale del riesame aveva ritenuto sussistenti i presupposti per l'utilizzo del captatore informatico, osservando che «Dal tenore letterale del primo decreto autorizzativo … risulta evidente come il P.M. avesse portato all'attenzione del Gip la sussistenza di elementi indiziari sufficienti a prospettare la sussistenza di delitti di criminalità organizzata [...]». In una simile ipotesi, secondo la decisione in esame, è ammissibile la riqualificazione giuridica dei fatti da parte di un giudice diverso da quello che ha disposto le intercettazioni al fine di affermare la sussistenza dei presupposti che permettono le operazioni captative mediante il cd. agente intrusore.

Il G.i.p., infatti, può dare una diversa qualificazione ai fatti sottoposti alla sua cognizione ai fini dell'autorizzazione di intercettazioni di comunicazione come concernenti reati di criminalità organizzata a norma dell'art. 13 d.l. 13 maggio 1991, n. 152, convertito dalla legge 12 luglio 1991, n. 203, anche se la richiesta del pubblico ministero fa esclusivo riferimento alla disciplina ordinaria di cui agli artt. 266 e 267 cod. proc. pen.[17]. Analogamente, non determina l'illegittimità del decreto autorizzativo delle operazioni di intercettazione la mancata specificazione della sussistenza di gravi indizi di reato con riferimento al ruolo di partecipe qualificato di cui all'art. 416, comma primo, cod. pen.[18], così chiaramente evidenziandosi, da parte della giurisprudenza, che non è assolutamente indispensabile una precisa qualificazione giuridica dei fatti nel provvedimento abilitativo all'attività captativa. Soprattutto, è stato ripetutamente affermato che l'omissione, nel decreto autorizzativo di intercettazioni per la durata di giorni quaranta, del riferimento ad uno dei reati di cui all'articolo 13 legge n. 203 del 1991, non rende inutilizzabili le intercettazioni, se dal complesso della motivazione si evince che esse avevano ad oggetto attività criminose organizzate[19].

---

[17] cfr. Cass. pen., Sez. 6, 21/07/2015, n. 34809, Gattuso, in *CED Cass*. n. 264447, nonché Cass. pen., Sez. 6, 22/11/2007, n. 47109, Alì, in *CED Cass*. n. 238715.

[18] cfr. Cass. pen., Sez. 2, 20/11/2009, n. 685, dep. 2010, Bronzini, in *CED Cass*. n. 246038, nonché Cass. pen., Sez. 5, 15/02/2000, n. 784, Terracciano, in *CED Cass*. n. 215730.

[19] così Cass. pen., Sez. 5, 11/11/2011, n. 3193, dep. 2012, Schettini, in *CED Cass*. n. 252988; Cass. pen., Sez. 4, 3/5/2007, n. 22511, Bleta, in *CED Cass*. n. 237028, ma anche, in termini sostanzialmente omogenei, Cass., Sez.

Questi arresti giurisprudenziali, secondo la Corte, si pongono certamente in linea con l'elaborazione delle Sezioni unite che, proprio in materia di motivazione dei provvedimenti autorizzativi di intercettazioni di conversazioni, distingue tra la "motivazione mancante o apparente" e quella semplicemente "difettosa"[20]. In particolare, la sentenza delle Sezioni unite" Primavera" del 2000, descrive la situazione di «difettosità» di motivazione come quella integrata da fattispecie «di incompletezza o insufficienza o non perfetta adeguatezza, ovvero di sovrabbondanza con ben probabili, in simili eccessi, slabbrature logiche; in una parola, di vizi che non negano e neppure compromettono la giustificazione, ma la rendono non puntuale. In tali casi il vizio va emendato dal giudice cui la doglianza venga prospettata, sia esso il giudice del merito, che deve utilizzare i risultati delle intercettazioni, sia da quello dell'impugnazione nella fase di merito o in quella di legittimità»[21].

Secondo il collegio, inoltre, la soluzione proposta trova una conferma di natura sistematica nella previsione di cui all'art. 597, comma 3, cod. proc. pen., che permette al giudice dell'impugnazione di merito di procedere ad una riqualificazione del fatto *ex officio*, anche dando una definizione giuridica più grave, né si pone in contrasto con il diritto di difesa o con la garanzia del contraddittorio, essendo la decisione del Tribunale del riesame sindacabile in sede di legittimità.

6. segue: la sentenza "Occhionero" del 2017.

La legittimità dell'uso del captatore informatico è poi stata oggetto della sentenza Cass., Sez. 5, 30/05/2017, n. 48370, Occhionero[22].

La vicenda ha tratto origine dalla denuncia presentata dal responsabile della sicurezza di una società pubblica il quale aveva ricevuto una *e-mail*, apparentemente inviata da uno studio legale, che conteneva in allegato un programma informatico capace di estrarre dati dal sistema informatico "bersaglio", superando i sistemi di protezione. Nel corso dell'inchiesta, sono state eseguite intercettazioni telematiche o informatiche, a loro volta per mezzo del captatore informatico. Quest'attività ha consentito di individuare, tra l'altro, alcuni *server* statunitensi nei quali erano memorizzati alcuni file abusivamente prelevati da computer in precedenza infettati dal predetto *software*. Il giudice delle indagini preliminari ha applicato la misura cautelare della custodia in carcere agli indagati per i reati di accesso abusivo ad un sistema informatico e telematico (art. 615-*ter* cod. pen.), aggravato dal danneggiamento di un sistema di interesse militare o di sicurezza pubblica nonché di intercettazione illecita di

5, 24/11/2009, n. 7023, dep. 2010, D'Angelo, in *CED Cass*. n. 246144.

[20] cfr., specificamente, Cass. pen., Sez. U, 21/06/2000, n. 17, Primavera, in *CED Cass*. n. 216665, nonché Cass. pen., Sez. U, 25/03/1998, n. 11, Manno, in *CED Cass*. n. 210610.

[21] Cass., Sez. unite, n. 17 del 21/06/2000.

[22] Su questa sentenza, volendo L. GIORDANO, *Intercettazioni: sì all'uso del trojan anche per reati diversi da quelli di criminalità organizzata*, in *Ilquotidianogiuridico.it*, 14 novembre 2017.

comunicazioni informatiche o telematiche (art. 617-*quater* cod. pen.) e di installazione di apparecchiature atte ad intercettare comunicazioni informatiche o telematiche (art. 617-*quinquies* cod. pen.), questi ultimi aggravati perché il sistema informatico colpito era utilizzato da un ente pubblico.

Avverso il provvedimento di conferma della custodia in carcere adottato dal Tribunale del riesame, gli indagati hanno proposto ricorso per cassazione, deducendo, tra l'altro, l'inutilizzabilità dei risultati delle intercettazioni effettuate mediante il captatore informatico. Secondo la prospettazione difensiva sarebbero stati violati i principi elaborati dalla sentenza Scurato, perché sarebbero state disposte intercettazioni in un luogo di privata dimora, e segnatamente nel computer fisso collocato nell'abitazione di uno degli indagati, pur se non si procedeva per un reato di criminalità organizzata. In ogni caso, non sarebbero state compiute intercettazioni telematiche riconducibili al paradigma dell'art. 266-*bis* cod. proc. pen., ma una perquisizione o un'ispezione del computer "bersaglio", «con acquisizione (sequestro) della copia o meglio della fotografia di un documento statico (*screenshot*) che compare a video o è prelevato».

La Corte ha ritenuto infondato il motivo di ricorso, affermando che la sentenza Scurato si riferisce solo all'impiego del captatore informatico per realizzare "intercettazioni tra presenti" ed aggiungendo che da essa non può essere tratto un principio generale estensibile anche a diverse forme di captazione. La portata dei principi espressi dalle Sezioni unite, pertanto, non può essere estesa alle ulteriori forme di intercettazione, tra cui quelle telematiche ex art. 266-*bis* cod. proc. pen. compiute in esame. Con una affermazione incidentale, poi, ha aggiunto che «il supremo organo nomofilattico non … ha escluso la legittimità dell'uso di tale strumento captativo per le intercettazioni tra presenti nei luoghi di privata dimora dove si stia svolgendo l'attività criminosa».

Parimenti infondato è stato ritenuto il motivo di ricorso nella parte in cui è stato prospettato che l'attività investigativa compiuta nel caso di specie esulerebbe dal novero delle intercettazioni.

La Corte, infatti, ha rilevato che le operazioni effettuate dalla polizia giudiziaria, «quanto meno in parte», sono consistite nella captazione in tempo reale di flussi informatici transitati sul computer dell'indagato, con acquisizione di dati contenuti nel computer, ovvero di flussi informatici transitati sui dispositivi. Si è quindi trattato di un'attività rientrante nel concetto di intercettazione, perché «dal provvedimento impugnato si ricava … che l'agente intrusore impiegato ha captato, comunque, anche un flusso di comunicazioni, richiedente un dialogo con altri soggetti, oltre a documentazione relativa ad un flusso unidirezionale di dati confinati all'interno dei circuiti del computer», secondo la distinzione proposta da una precedente sentenza della medesima Corte di Cassazione[23]. Tale accertamento, secondo la Corte, rende irrilevante affrontare la questione della qualificazione giuridica dell'attività realizzata e, specificamente se l'acquisizione dei dati presenti nell'*hard disk* del computer costituisca

[23] Cass., Sez. 5, 14/10/2009, n. 16556, dep. 2010, Virruso, in *CED Cass*. n. 245954.

intercettazione oppure se integri una prova atipica ovvero, ancora, se richieda un provvedimento di perquisizione e sequestro (che, peraltro, nel caso di specie era stato impedito dalla condotta degli imputati che, avvedutisi dell'intervento della polizia giudiziaria per mezzo di un sistema di video-sorveglianza, hanno bloccato il funzionamento delle loro apparecchiature elettroniche, rifiutandosi poi di fornire le *password* di accesso).

L'irrilevanza della questione, inoltre, è derivata anche da un'altra ragione.

Il ricorrente, infatti, non ha ottemperato all'onere di precisare, in ossequio al principio di specificità delle impugnazioni, quali dati captati tramite *trojan* fossero eventualmente colpiti dalla sanzione dell'inutilizzabilità, omettendo di chiarirne la decisività in riferimento al provvedimento impugnato, che è fondato anche su altri elementi indiziari[24].

7. segue: la sentenza "Schirripa" del 2017.

Il tema della legittimità dell'uso del captatore informatico nelle indagini è stato oggetto anche della sentenza Cass., Sez. 1, 28/06/2017, n. 29169, Schirripa[25].

Nel corso delle indagini relative all'omicidio del Procuratore della Repubblica presso il Tribunale di Torino, dott. Bruno Caccia, in particolare, sono state disposte intercettazioni tra presenti a mezzo di inoculazione di virus informatico nell'apparecchio cellulare in uso ad un indagato. Con il ricorso per cassazione avverso il provvedimento del Tribunale del riesame che aveva confermato la misura cautelare della custodia in carcere per concorso in omicidio premeditato, è stato dedotta, tra l'altro, inutilizzabilità dei risultati di queste captazioni.

La Corte ha rigettato questo motivo di ricorso, rimarcando la legittimità dell'impiego dell'agente intrusore perché, nel caso di specie, sia la richiesta di intercettazioni del pubblico ministero, che il provvedimento autorizzativo del Gip, avevano dato atto della matrice mafiosa del delitto. Le captazioni, pertanto, erano state autorizzate ex art. 13 del d.l. n. 152 del 1991, nel pieno rispetto dei principi elaborati dalla pronuncia delle Sezioni unite illustrata in precedenza.

La disciplina speciale per le intercettazioni relative a reati di criminalità organizzata, più specificamente, in ragione della sua natura processuale, deve trovare applicazione anche per le indagini relative a reati commessi prima della sua introduzione, come appunto l'omicidio del dott. Caccia avvenuto il 26 giugno 1983. In forza della regola *tempus regit actum*, infatti, la disciplina e la validità di un atto dipende dalla sua conformità alla disciplina vigente nel momento in cui è stato formato e non a quella vigente all'epoca del fatto – reato.

---

[24] Cass. pen., Sez. U, 23/04/2009, n. 23868, Fruci, in *CED Cass*. n. 243416.

[25] Su questa sentenza, volendo, L. GIORDANO, *Le prime applicazioni della sentenza "Scurato" nella giurisprudenza di legittimità. La legge n. 103 del 2017*, in *Cass. pen.* 2018, suppl. 4, 343.

8. segue: La sentenza "Romeo" del 2018.

Indicazioni giurisprudenziali molto significative sul tema in esame si possono trarre anche dalla sentenza Cass., Sez. 6, 8/03/2018, n. 45486, Romeo[26]. Anche in questo caso, relativo ad una vicenda che verosimilmente è una costola del precedente giudizio in cui è stata emessa la sentenza del 2017 dapprima illustrata, la difesa, ricorrendo per cassazione avverso un'ordinanza cautelare, ha eccepito l'inutilizzabilità dei risultati delle intercettazioni realizzate mediante *trojan*.

La Corte ha ribadito che la motivazione del decreto autorizzativo assolve ad una ineliminabile funzione di garanzia, perché, attraverso essa, deve essere esplicitato il collegamento tra l'indagine e la persona le cui comunicazioni si intendono intercettare. Nella motivazione del decreto che autorizza l'impiego del captatore informatico, inoltre, occorre che sia evidenziato che la qualificazione, pure provvisoria del fatto come inquadrabile in un contesto di criminalità organizzata, risulti ancorata a sufficienti, sicuri e obiettivi elementi indiziari.

La decisione, peraltro, si segnala perché invita a distinguere il caso in cui il destinatario della intercettazione sia un soggetto indagato da quello in cui l'intercettato sia una persona terza, non indagata. In tale ultima ipotesi, infatti, la necessità di motivare la correlazione tra l'indagine in corso e l'intercettato è oltremodo maggiore; in tali casi, oltre alla verifica relativa alla base indiziaria oggettiva, «è necessario che il giudice indichi ed espliciti chiaramente l'interesse investigativo sottostante, chiarisca cioè le ragioni di collegamento diretto o indiretto (conoscenza) tra il soggetto ed il fatto di reato oggetto di accertamento; è necessario che si indichino i motivi per i quali il soggetto terzo che si intende intercettare dovrebbe essere "informato sui fatti" e perché si ritiene che vi possano essere conversazioni o comunicazioni attinenti a quei fatti».

Nella medesima sentenza, inoltre, la Corte ha affermato che la modifica delle modalità esecutive delle captazioni, concernendo un aspetto meramente tecnico, può essere autonomamente disposta dal pubblico ministero, non occorrendo un apposito provvedimento da parte del giudice per le indagini preliminari. Sono state ritenute utilizzabili, pertanto, le intercettazioni acquisite tramite la collocazione di microspie anziché mediante l'impiego di un software spia, così come disposto nel decreto autorizzativo del giudice. In questo modo, la Corte ha ribadito che l'impiego del captatore costituisce soltanto una modalità esecutiva delle intercettazioni "tra presenti".

9. segue: la sentenza "Chianchiano ed altri" del 2019.

Da ultimo merita un riferimento la sentenza Cass., Sez. 1, 25/06/2019, n. 50972, Chianchiano ed altri, che ha specificamente affrontato uno dei principali profili di critica sollevati dalla dottrina nei confronti della sentenza "Scurato"[27].

---

[26] Su questa sentenza si veda M. TORRE, *Intercettazioni tra presenti mediante captatore informatico. La S.C. sulla motivazione del decreto autorizzativo*, in *Il Penalista*, 19 novembre 2018.

[27] Su questa sentenza, volendo L. GIORDANO, *Captatore informatico: inutilizzabili i risultati delle intercettazioni*

In particolare, proponendo ricorso per cassazione avverso una sentenza di condanna per i reati di omicidio e di porto e detenzione di armi da guerra e di minaccia aggravata dall'uso di armi, gli imputati hanno dedotto, tra l'altro, l'inutilizzabilità dei risultati delle intercettazioni realizzate nel corso delle indagini per mezzo del captatore informatico installato nello *smartphone* di un familiare della vittima, in un caso in cui il decreto autorizzativo limitava le intercettazioni solo ai dialoghi che sarebbero intervenuti in luogo pubblico.

La Corte ha rilevato che la disciplina dell'utilizzo del captatore si ravvisa negli art. 266, comma 2, cod. proc. pen. e nell'art. 13 del d.l. citato, come interpretati dalla sentenza delle Sezioni unite Scurato.

Dopo questa sentenza, invero, è intervenuta la riforma della disciplina delle intercettazioni ad opera del d.lgs. n. 216 del 2017, che ha riguardato anche la disciplina del captatore informatico. L'applicazione delle innovazioni, però, pur entrate in vigore, è stata via via prorogata ai sensi dell'art. 9, comma 1, dello stesso d.lgs. e successive modificazioni.

L'unica precisazione, seppur meramente incidentale perché relativa a questione non rilevante nel caso in esame come ha osservato la stessa decisione in commento, riguarda i delitti dei pubblici ufficiali contro la pubblica amministrazione, ai quali si applica, per effetto dell'art. 6, comma 1, d.lgs. n. 216 del 2017, la disciplina dell'art. 13 d.l. 13 maggio 1991, n. 152, conv. con mod. nella legge 12 luglio 1991, n. 203. Questa norma, secondo la sentenza in esame, sarebbe immediatamente operativa («il rinvio alla norma anzidetta renderebbe a regime la nuova disciplina e di operatività immediata il relativo statuto regolatore», così si esprime la sentenza).

Nel caso di specie, il giudice per le indagini preliminari aveva emesso due decreti autorizzativi, stabilendo le condizioni d'applicazione del captatore informatico come microspia e, segnatamente, escludendo i domicili privati dai luoghi in cui lo strumento poteva essere adoperato. Secondo il Gip, sarebbe stato possibile accertare preventivamente la modalità di impiego delle captazioni, sfruttando la connessione dati e la localizzazione GPS. Trattandosi di reato diverso da quelli di criminalità organizzata, l'uso dello strumento informatico era stato sottoposto alla condizione che le conversazioni captate non avvenissero in luogo di privata dimora.

Valorizzando proprio tale profilo, nella sentenza di appello sono state ritenute utilizzabili due conversazioni, registrate, rispettivamente, in un'automobile e sulla pubblica via.

La Corte di cassazione non ha condiviso questa interpretazione.

Sulla scorta della sentenza selle Sezioni unite "Scurato", è stato rilevato che, nell'autorizzare le intercettazioni per mezzo del captatore informatico, il giudice non ha la possibilità di predeterminare i luoghi in cui avverrà l'intercettazione, attesa la natura portatile dello strumento impiegato. Esso, in altri termini, condiziona l'impiego della tecnologia, poiché è suscettibile per sua struttura e finalità, di svolgere un modello di

---

per la prova di reati diversi da quelli di criminalità organizzata, in *Il penalista*, 13 gennaio 2020.

intercettazione aperta, con carattere itinerante e privo sostanzialmente di ogni limitazione.

A ciò va aggiunto che, là dove uno dei due interlocutori sia a conoscenza della captazione e collabori in fase di esecuzione, «residuerebbe ampia possibilità di influire anche sul risultato "acquisitivo" accedendo o spegnendo l'apparecchio o isolando la cd. *local positioning*», con la conseguente reale impossibilità di comprendere ove l'intercettazione è stata eseguita.

In ogni caso, «il rischio sarebbe quello di acquisire informazioni e conversazioni anche in luoghi di privata dimora, in violazione non solo del provvedimento giudiziale di autorizzazione, ma della stessa disposizione di legge che ne regolamenta l'attuazione».

Ne consegue, secondo la decisione in commento, «la necessità di offrire un'interpretazione rigorosa della disposizione che esclude *ab origine* la possibilità di ammettere l'intercettazione delle conversazioni, a mezzo di captatore informatico, in difetto del fondato motivo che nei luoghi di cui all'art. 614 cod. pen. si stia svolgendo attività delittuosa, in ambito di delitti diversi da quelli di criminalità organizzata».

Non è ammissibile, inoltre, un controllo postumo funzionale alla verifica d'utilizzabilità. La valutazione di legittimità non potrebbe essere operata *ex post*, attraverso una verifica con effetto legittimante postumo, tale da indurre una legalizzazione "successiva" dei risultati delle captazioni, a fronte di una materia in cui l'intercettazione deve, piuttosto, risultare legittima, sin dalla sua genesi e dal provvedimento che la autorizza.

Secondo la decisione in commento, «nella specifica vicenda si discuterebbe di intercettazioni realizzate in difetto di una previsione normativa espressa e si aprirebbero rischi evidenti, in punto di lesione dei diritti di libertà, oggetto di presidio costituzionale». Ne deriva che «le intercettazioni per delitti diversi da quelli di criminalità organizzata, nel quadro normativo vigente non possono essere eseguite nei luoghi di privata dimora, per mezzo del captatore informatico, se non vi sia fondato motivo di ritenere che ivi sia in corso attività criminosa».

Nella specifica vicenda, pertanto, la Corte ha ritenuto che le intercettazioni acquisite con captatore informatico non sono conformi allo statuto normativo e vanno espunte dal materiale probatorio a carico degli imputati.

La sentenza, peraltro, ha ritenuto che il quadro dimostrativo della responsabilità degli imputati resistesse, nonostante l'espunzione dal materiale probatorio dei colloqui indicati, confermando la decisione di condanna impugnata.

10. L'uso del captatore per la funzione di "*Keylogger*".

1. Appare opportuno integrare l'illustrazione del panorama giurisprudenziale sul tema del captatore informatico con il riferimento ad una pronuncia che, pur non affrontando direttamente la questione della legittimità del suo impiego, ha ritenuto corretto il suo utilizzo per uno scopo particolare.

Si allude alla Cass., Sez. 4, 28/06/2016, n. 40903, Grassi, relativo ad una vicenda in cui il captatore sembra essere stato impiegato con una sorta di funzione di "*Keylogger*"[28].

Nel corso di un'indagine relativa ad un'organizzazione che importava ingenti quantitativi di cocaina dal Sud-America è stata captata la corrispondenza elettronica di diversi imputati[29]. Le e-mail, in particolare, sono state oggetto di un provvedimento d'intercettazione di flussi telematici in entrata e in uscita dai computer ubicati nei predetti *internet point* ai sensi dell'art. 266-*bis* cod. proc. pen. Le comunicazioni lasciate in "bozza" e quelle che erano state inviate o ricevute in precedenza, ma giacenti nelle diverse cartelle dell'*account* sono state carpite con un sistema più ingegnoso: gli investigatori si sono procurati le credenziali di accesso controllando a distanza gli imputati tramite un virus informatico del tipo *trojan* che, inoculato nei computer, ha permesso di conoscere quanto veniva digitato sulla tastiera; quindi, sono entrati direttamente nelle caselle di posta elettronica, apprendendone il contenuto.

La Corte ha ritenuto che le e-mail pervenute o inviate al destinatario e archiviate nelle cartelle della posta elettronica (cioè "parcheggiate") possono essere oggetto di intercettazione, trattandosi di un flusso di dati già avvenuto ed essendo irrilevante la mancanza del presupposto della loro apprensione contestualmente alla comunicazione. Esulano, invece, dal materiale intercettabile le *e-mail* "bozza", non inviate al destinatario", ma conservate nell'*account* di posta (o in apposito spazio virtuale come *Dropbox* o *Google Drive*), le quali possono comunque essere acquisite per mezzo di un sequestro di dati informatici.

Tra i vari spunti che la decisione suscita, in questo contesto merita di essere approfondito l'impiego del virus del tipo cd. *trojan*. Secondo la sentenza, «l'uso del *trojan* … è stato limitato … all'acquisizione delle password di accesso agli account di posta elettronica. Ottenute queste password, gli inquirenti hanno avuto anch'essi accesso ai vari account nomeutente@hotmail.com e hanno preso visione: a) dei messaggi che venivano via via inviati o ricevuti; b) dei messaggi che venivano salvati nella cartella "bozze"». Di conseguenza, «si è usato il programma informatico … così come si è da sempre usata la microspia per le intercettazioni telefoniche o ambientali»[30].

---

[28] Su questa sentenza sia consentito il rinvio a L. Giordano, *L'intercettazione delle e-mail (già) ricevute o inviate e l'acquisizione di quelle parcheggiate nella cartella "bozze"*, in *www.ilpenalista.it*, Milano, 14 novembre 2016

[29] Più specificamente, durante le investigazioni, per mezzo di servizi di pedinamento e osservazione, era stato appurato che gli imputati frequentavano alcuni *internet point* di Roma per accedere ad alcune caselle di posta elettronica attivate presso il *provider* statunitense "*hotmail.com*", con le quali intrattenevano una corrispondenza con i complici sudamericani. I contatti informatici avvenivano secondo due diverse modalità. In alcuni casi, i messaggi di posta erano normalmente spediti in via telematica; in altri, invece, venivano scritte *e-mail* che non erano inoltrate al destinatario, ma archiviate nella cartella "bozze". Esse potevano essere lette dai complici che, in possesso di *username* e *password*, accedevano successivamente alla casella di posta elettronica. Questo singolare modo di comunicare era impiegato soprattutto per le informazioni più riservate, come quelle che avevano ad oggetto i numeri telefonici "dedicati" allo svolgimento delle singole operazioni di importazione di droga.

[30] La soluzione accolta da questa sentenza potrebbe essere posta in discussione. Non sembrerebbe, invero, che il software sia stato adoperato per cogliere comunicazioni, quanto piuttosto per individuare ciò che era digitato sul computer. In questo modo sono state acquisite le *password* che hanno consentito l'accesso agli *account* di posta elettronica ed alle mail contenute. Appare arduo ricomprendere la digitazione sulla tastiera

Da questa decisione traspare come non sia sempre agevole comprendere quale uso del mezzo tecnologico sia stato fatto in concreto nella specifica indagine. Tale accertamento è il presupposto indispensabile per procedere alla relativa qualificazione giuridica[31].

2. Per mera completezza, considerato il riferimento al delicato tema dell'acquisizione delle mail compiuto dalla sentenza appena illustrata, appare utile illustrare brevemente anche un'altra decisione. Si allude a Cass., Sez. 6, 28/06/2019, n. 28269, Pizzarotti, secondo cui «è legittimo il sequestro probatorio di messaggi di posta elettronica già ricevuti o spediti e conservati nelle caselle di posta del computer, in quanto tali comunicazione hanno natura di documenti ai sensi dell'art. 234 cod. proc. pen. e la relativa acquisizione non soggiace alla disciplina delle intercettazioni telefoniche ex art. 266 e ss. cod. proc. pen., la quale postula la captazione di un flusso di comunicazioni in atto»[32].

Secondo questa decisione, i dati informatici rinvenuti in un server o in un personal computer, anche se consistenti in messaggi di posta elettronica "scaricati" e conservati nella memoria fisica dell'apparecchio elettronico, sono qualificabili come documenti ai sensi dell'art. 234 cod. proc. pen.

La relativa attività di acquisizione processuale, pertanto, non soggiace alle regole stabilite per la corrispondenza, né tantomeno alla disciplina delle intercettazioni.

L'attività di intercettazione, infatti, presuppone per sua natura la captazione di un flusso di comunicazioni nel momento stesso in cui si realizza.

Nel caso di specie, invece, il provvedimento di sequestro probatorio è intervenuto per acquisire *ex post* i dati risultanti da comunicazioni già avvenute e conservate nella memoria fisica del computer. L'apprensione, pertanto, ha riguardato il risultato di una comunicazione, già definita e non più modificabile, che è stata eseguita

---

di un computer necessaria per accedere ad una casella di posta elettronica nel concetto di comunicazione. Sembra pertanto che il software sia stato usato per compiere un'ispezione o una perquisizione, di tipo elettronico, che ha condotto all'acquisizione (sequestro) della *password*, attività con le quali la sentenza "Scurato" non si è confrontata. In dottrina è stato evidenziato che il captatore, consentendo l'accesso diretto al dispositivo infettato dalla prospettiva del suo utilizzatore, è in grado di assicurare l'acquisizione intellegibile degli scambi di corrispondenza che, ove coperti di cifratura, non sarebbe possibile ottenere con la classica intercettazione *in itinere* del flusso informatico. Tale caratteristica, unitamente alle altre utilità desumibili dal ricorso a questo mezzo di investigazione, inducono a ritenere ravvisabile il controllo occulto e continuativo come categoria probatoria (F. NICOLICCHIA, *Il controllo occulto e continuativo come categoria probatoria: premesse teoriche di una sistemazione*, in *Dir. pen. cont. – Riv. trim.*, 2019, 2, 435).

[31] Sul tema si veda E.M. MANCUSO, *Le acquisizioni mediante captatore non disciplinate dalla legge*, in A. Giarda, F. Giunta, G. Varraso (a cura di), *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, Padova, 2018, 193 e ss., in particolare il par. 4, intitolato "*perquisizioni on line e prova atipica*"; L. PARLATO, *Problemi insoluti: le perquisizioni on-line*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 289 e ss.

[32] Su questa sentenza, volendo, L. GIORDANO, *Acquisizione dei messaggi di posta elettronica già ricevuti o spediti. I chiarimenti della Cassazione sulla disciplina da applicare*, in *Il penalista*, Milano, 30 settembre 2019. Sull'intercettazione delle mail si veda M. TORRE, l'intercettazione di flussi telematici, in Cadoppi, Canestrari, Manna (a cura di), *Cybercrime*, Milano, 2019, 1466 e ss.

con lo strumento informatico. In ragione della finalità probatoria, essa è sottoposta alla disciplina del sequestro, applicabile rispetto ad azioni di comunicazione ormai esaurite.

11. Il decreto legislativo n. 216 del 2017: La riforma dell'art. 266 cod. proc. pen. e l'uso del "captatore informatico" per le indagini relative ai delitti dei pubblici ufficiali contro la pubblica amministrazione.

In attuazione dei criteri contenuti nell'art. 1, comma 84, lett. e), della legge n. 103 del 2017[33], è stato adottato il d.lgs. 29 dicembre 2017, n. 216, che ha disciplinato, nell'ambito della riforma delle intercettazioni, l'utilizzo nelle indagini del captatore informatico e l'uso processuale del materiale probatorio così raccolto[34].

L'art. 4 del d.lgs. n. 216 del 2017, in particolare, ha fissato i limiti di ammissibilità delle intercettazioni tra presenti tramite captatore informatico. Questa disposizione ha modificato l'art. 266, comma 2, cod. proc. pen. con l'inserimento delle seguenti parole: ", *che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile*".

Dopo il comma 2 della medesima norma, inoltre, è stato inserito un nuovo comma 2-*bis* in forza del quale "*L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, comma 3-bis e 3-quater*".

Per effetto di questa riforma, sul piano dei limiti di ammissibilità dello strumento in esame:

– l'art. 266, comma 2, cod. proc. pen. rimane la disposizione che regola i presupposti di ammissibilità delle intercettazioni "tra presenti", le quali possono essere realizzate non solo tramite strumenti tradizionali, ma anche sfruttando le potenzialità del "captatore informatico". La nuova legge, dunque, ha preso atto che quest'ultimo integra solo una particolare modalità tecnica per la realizzazione dell'intercettazione delle conversazioni tra presenti;

---

[33] Sulla delega per l'adozione di un decreto legislativo che disciplini le intercettazioni per mezzo del captatore informatico si vedano, tra gli altri, E. TURCO, *La ricerca della prova ad alta efficacia intrusiva: il captatore elettronico*, 307 e ss., in A. Scalfati (a cura di), *La riforma della giustizia penale, Commento alla legge 23 giugno 2017, n. 103*, Torino, 2017; M. GIALUZ, A. CABIALE, J. DELLA TORRE, *Riforma Orlando: le modifiche attinenti al processo penale, tra codificazione della giurisprudenza, riforme attese da tempo e confuse innovazioni*, in *Dir. pen. cont*. – *Riv. trim.*, 2017, 3, 194 e ss.; C. PARODI, *La riforma "Orlando": la delega in tema di "captatori informatici"*, in *www.magistraturaindipendente.it*. 4 aprile 2017; volendo, L. GIORDANO, *La delega per la disciplina delle intercettazioni tra presenti mediante immissione di captatori informatici*, in A. Marandola, T. Bene, *La riforma della giustizia penale*, Milano, 2017, 396.

[34] Sulle norme in tema di captatore informatico previste dal d.gs. n. 216 del 2017, tra gli altri, si veda G. DI PAOLO, *Le intercettazioni mediante l'uso di captatore informatico*, in A. Giarda, F. Giunta, G. Varraso (a cura di), *Dai decreti attuativi della legge "Orlando" alle novelle di fine legislatura*, Padova, 2018, 165 e ss. Per una valutazione delle principali questioni, tra gli altri, si veda T. BENE, *Il re è nudo: anomie disapplicative a proposito del captatore informatico*, in *Arch. pen*. 2019, 3, 7.

– sia che la captazione delle conversazioni avvenga con strumenti consueti, sia che si utilizzi il "captatore informatico", quando le intercettazioni sono compiute in un luogo qualificabile come domicilio, occorre che sia in corso l'attività criminosa;

– in forza del nuovo art. 266, comma 2-*bis*, cod. proc. pen., nella versione originariamente introdotta dal d.lgs. n. 216 del 2017, per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, cod. proc. pen., l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile "*è sempre consentita*", potendo prescindersi, pertanto, dal presupposto dello svolgimento in corso dell'attività criminosa anche qualora il mezzo di ricerca della prova fosse attivato nei luoghi indicati dall'art. 614 cod. pen.;

– per i reati che non sono ricompresi nell'elenco contenuto negli artt. 51, comma 3-*bis* e 3-*quater* cod. proc. pen. (catalogo diverso da quello di cui all'art. 13 d.l. n. 151 del 1991, perché, ad esempio, non contiene il reato di cui all'art. 416 cod. pen.), invece, l'impiego del mezzo tecnologico anche in un domicilio è comunque permesso, ma solo quando è stata raggiunta la prova che nell'abitazione sia in corso lo svolgimento di un'attività illecita;

– dal tenore della nuova disposizione, inoltre, pare possa desumersi che è ammissibile l'utilizzo del programma informatico al fine di compiere intercettazioni ambientali in luoghi pubblici o aperti al pubblico per le indagini relative a tutte le fattispecie penali per le quali l'art. 266 cod. proc. pen. consente le intercettazioni[35].

L'art. 1, comma 84, lett. *d*), della legge n. 103 del 2017, inoltre, ha delegato il Governo ad adottare prescrizioni volte alla 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»[36].

Il legislatore ha attuato la delega con l'art. 6 del d.lgs. n. 216 del 2017, che ha operato in una duplice direzione:

– l'art. 6, comma 1, del d.lgs. n. 216 del 2017 ha esteso la disciplina speciale prevista per i reati di criminalità organizzata dall'art. 13 del d.l. n. 151 del 1991 anche alle indagini per tali delitti. Il presupposto per lo svolgimento di intercettazioni, pertanto, non è più rappresentato dalla "gravità" indiziaria di un reato che rientra nella suddetta categoria, ma dalla mera "sufficienza" di tale base indiziaria. La durata dell'autorizzazione è fissata in quaranta giorni (e non in quindici, come nel caso di

---

[35] Va osservato che la nuova disciplina è esplicitamente circoscritta all'installazione del captatore "*su un dispositivo elettronico portatile*". Il legislatore, seguendo alla lettera le indicazioni contenute nella legge delega, infatti, ha fatto riferimento a programmi informatici inoculati in uno *smartphone* o in un *tablet*, preoccupato dall'ingresso dello *smartphone* in ambienti aventi natura domiciliare.

[36] L'art. 266, comma 1, lett. b), cod. proc. pen., in verità, già prevedeva una semplificazione per l'accesso alle intercettazioni nel caso di reati contro la pubblica amministrazione, stabilendo che esse sono consentite per delitti per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni (e non superiore nel massimo a cinque anni, come avviene per gli altri delitti). Su questo criterio contenuto nella legge delega sia consentito il rinvio a L. GIORDANO, *La delega per la riforma della disciplina delle intercettazioni*, in A. Marandola, T. Bene (a cura di), *La riforma della giustizia penale*, Milano, 2017, 382 e ss.

procedura ordinaria), mentre quella delle successive proroghe in venti giorni (e non quindici);

– l'art. 6, comma 2, del medesimo d.lgs., tuttavia, ha limitato l'applicazione della disciplina prevista per i reati di criminalità organizzata in modo rilevante, escludendo l'applicazione della deroga alla condizione di cui all'art. 266, comma 2, cod. proc. pen. per le captazioni in luoghi domiciliari. L'impiego nelle indagini del "captatore informatico" in ambienti qualificabili come domicilio ai sensi dell'art. 614 cod. pen., anche per la ricerca della prova dei più gravi reati contro la pubblica amministrazione, presuppone che l'attività criminosa sia in corso.

La norma, in verità, suscita alcuni dubbi interpretativi.

La sua area operativa, infatti, è delimitata con riferimento ai "*procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni*".

Una lettura rigorosa di essa condurrebbe a ritenere che gli standard più blandi rispetto a quelli ordinari che sono richiesti per l'impiego delle intercettazioni in tema di criminalità organizzata sono stati estesi alle investigazioni che riguardano i delitti di cui al Capo I – intitolato appunto "*Dei delitti dei pubblici ufficiali contro la pubblica amministrazione*" – del Titolo II del Libro II del codice penale. Si tratta dei reati compresi tra gli artt. 314 e 335-*bis* cod. pen. Esulerebbero dal raggio di azione della norma citata, pertanto, fattispecie come la turbata libertà degli incanti (art. 353 cod. pen.) e la turbata libertà del procedimento di scelta del contraente (art. 353-*bis* cod. pen.)[37].

Una diversa lettura potrebbe fare riferimento, nell'ambito dei delitti contro la pubblica amministrazione di cui al titolo II del libro II del codice penale, ai reati posti in essere da soggetti che hanno la qualifica di pubblici ufficiali, con esclusione di quelli relativi, agli incaricati di pubblico servizio.

Su questo specifico punto ha inciso, come meglio si vedrà nel prosieguo, il d.l. 30 dicembre 2019, n. 161, il cui esame, peraltro, esula dal perimetro del presente scritto.

12. I tempi di applicazione del d.lgs. n. 216 del 2017 di riforma della disciplina delle intercettazioni.

L'art. 9 del d.lgs. n. 216 del 2017 contiene una disposizione transitoria che regola l'efficacia nel tempo della riforma.

Essa originariamente prevedeva che le disposizioni di cui agli articoli 2, 3 4, 5 e 7 – dunque anche quelle illustrate che regolamentano l'uso del captatore informatico – si applicassero alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il centottantesimo giorno successivo alla data di entrata in vigore del decreto legislativo stesso, cioè a partire dal 26 luglio 2018 (mentre quella di cui all'art. 2,

[37] Per tali reati è prevista una pena edittale massima fino a 5 anni di reclusione e, quindi, rientrano nelle condizioni previste dall'art. 266, comma 1, lett. b), cod. proc. pen.

comma 1, lettera b), relativa alla pubblicazione dell'ordinanza cautelare, decorsi dodici mesi dalla data di entrata in vigore del decreto)[38].

La data indicata è stata successivamente differita.

Ai sensi dell'art. 2, comma 1, del d.l. 25 luglio 2018, n. 91, convertito, con modificazioni, dalla legge 21 settembre 2018, n. 108, infatti, è stato stabilito che le suddette disposizioni si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 marzo 2019.

In seguito, la legge 30 dicembre 2018, n. 145, c.d. legge di bilancio, ha prorogato al 1 agosto 2019 l'applicazione di queste norme[39]; poi, ancora, è stato stabilito dall'art. 9, comma 2, lett. a), del d.l. 14 giugno 2019, n. 53, convertito, con modificazioni, dalla legge 8 agosto 2019, n. 77, che queste norme si applicano alle operazioni di intercettazioni relative ai provvedimenti autorizzativi emessi dopo il 31 dicembre 2019.

La sola norma della riforma entrata in vigore all'esito dell'ordinario termine dalla pubblicazione avvenuta in data 11 gennaio 2018, pertanto, è quella di cui all'art. 6, che concerne la descritta semplificazione delle condizioni per l'impiego delle intercettazioni nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione (su questa norma, come si vedrà meglio in seguito, è intervenuta la nuova legge "anticorruzione").

Sulla disposizione che regola l'efficacia della riforma, infine, è intervenuto il d.l. 30 dicembre 2019, n. 161, convertito con modificazioni dalla legge n. 7 del 2020, il cui esame esula dal perimetro del presente scritto. L'art. 1 di tale decreto legge, infatti, dispone che la riforma si applichi ai "*ai procedimenti penali iscritti dopo il 30 aprile 2020*".

13. La nuova legge "anticorruzione" e l'uso del captatore informatico per i reati del pubblici ufficiali contro la pubblica amministrazione: l'abrogazione dell'art. 6, comma 2, d.lgs. n. 216 del 2017.

In attesa della maturazione del termine per l'applicazione della legge di riforma della disciplina delle intercettazioni, che progressivamente è stato differito, il legislatore è intervenuto nuovamente nella materia.

L'art. 1 della legge 9 gennaio 2019, n. 3, recante "*Misure per il contrasto dei reati contro la pubblica amministrazione nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*", è intervenuto sulla disciplina delle intercettazioni compiute tramite captatore informatico con due disposizioni.

L'art. 1, comma 3, di tale legge, in primo luogo, ha disposto l'abrogazione dell'art. 6, comma 2, del d. lgs. 29 dicembre 2017, n. 216. È stata abrogata, pertanto, la norma della riforma delle intercettazioni che escludeva l'uso del captatore per realizzare

[38] M. GAMBARDELLA, *Entrata in vigore e profili di diritto transitorio, in Nuove norme in tema di intercettazioni*, in G. Giostra, R. Orlandi (a cura di), *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, Torino, 2018, 160.

[39] Sul rinvio si veda L. FILIPPI, *Una (provvidenziale) nuova proroga in materia di intercettazioni*, in *Il penalista*, 8 gennaio 2019.

intercettazioni nei luoghi indicati dall'art. 614 cod. pen. in mancanza del fondato motivo che ivi fosse in corso l'attività criminosa.

Il risultato perseguito è l'estensione dell'intera disciplina delle intercettazione di criminalità organizzata prevista dall'art. 13 del d.l. n. 152 del 1991, convertito nella legge n. 203 del 1991 ai procedimenti relativi ai reati dei pubblici ufficiali contro la pubblica amministrazione.

Più precisamente, l'intercettazione tra presenti può essere eseguita nei luoghi indicati dall'art. 614 cod. pen. – e cioè nelle abitazioni o in altri luoghi di privata dimora – anche quando non ricorre il requisito aggiuntivo richiesto dall'art. 266, comma 2, cod. proc. pen. e, cioè, l'attività criminosa in corso nell'ambiente domiciliare[40].

Il presupposto per lo svolgimento di intercettazioni è rappresentato dalla mera "sufficienza" della base indiziaria raccolta e dalla necessità dello strumento. La durata dell'autorizzazione è fissata in quaranta giorni, mentre quella delle successive proroghe in venti giorni.

L'art. 1, comma 3, della legge 9 gennaio 2019, n. 3, è entrato in vigore in data 31 gennaio 2019.

14. segue: Le modifiche alle norme del codice di rito che disciplinano le intercettazioni.

Il successivo art. 1, comma 4, della legge 3 del 2019, poi, ha apportato alcune modifiche alle disposizioni del codice di rito in tema di intercettazioni – e segnatamente agli artt. 266 e 267 cod. proc. pen. – finalizzate a permettere un più ampio ricorso al captatore informatico nelle indagini per i reati contro la pubblica amministrazione.

Sono state modificate, in particolare, alcune disposizioni introdotte dall'art. 4 del d.lgs. n. 216 del 2019, la cui applicazione, come si è visto, è stata differita (attualmente ai provvedimenti che autorizzano intercettazioni emessi dopo il 31 dicembre 2019).

Precisamente:

a) con l'art. 1, comma 4, lett. a), all'art. 266, comma 2-*bis*, cod. proc. pen. sono state aggiunte, in fine, le seguenti parole: "*, e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4*".

Per effetto di questo intervento normativo, in forza dell'art. 266, comma 2-*bis*, cod. proc. pen., l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile "*è sempre consentita*" non solo per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, cod. proc. pen., ma anche per quelli dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni. Anche per questi reati, pertanto, essendo "*sempre consentita*" l'intercettazione mediante il captatore, si può prescindere

[40] È stata abrogata, in altri termini, la norma speciale relativa al "captatore informatico su dispositivo elettronico portatile" che derogava al regime di ammissibilità delle intercettazioni fissato dall'art. 6, comma 1, del d.lgs. n. 216 del 2017, che, a sua volta, deroga al più restrittivo regime di cui all'art. 266 cod. proc. pen.

dal presupposto dello svolgimento in corso dell'attività criminosa qualora il mezzo di ricerca della prova sia attivato in un luogo di cui all'art. 614 cod. pen., richiesto dal precedente art. 266, comma 2, cod. proc. pen.;

b) l'art. 1, comma 4, lett. b), della legge 3 del 2019, poi, ha inserito all'art. 267, comma 1, terzo periodo, dopo le parole: "*all'articolo 51, commi 3-bis e 3-quater*", le seguenti: "*e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4,*".

La norma che ne deriva è la seguente: "*1. Il pubblico ministero richiede al giudice per le indagini preliminari l'autorizzazione a disporre le operazioni previste dall'art. 266. L'autorizzazione è data con decreto motivato quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini. Il decreto che autorizza l'intercettazione tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile indica le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini; nonché, se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4, i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono*".

Per illustrare il senso di questa modifica normativa, la cui formulazione letterale potrebbe risultare ambigua, occorre precisare che l'art. 267 cod. proc. pen., così come riformato dal d.lgs. n. 216 del 2017, obbliga il giudice a compiere uno sforzo motivazionale nell'adottare il provvedimento che autorizza lo svolgimento di intercettazioni per mezzo del captatore informatico.

In tale atto, infatti, devono essere indicate le ragioni che rendono necessaria tale modalità in relazione allo svolgimento delle indagini nonché il luogo ed il tempo ove è consentita l'attivazione del microfono. Il giudice deve adeguatamente motivare nel decreto autorizzativo in ordine alla modalità di captazione prescelta ed indicare gli "ambienti" in cui la stessa dovrà avvenire, «secondo un verosimile progetto investigativo che implica l'individuazione anche in forma indiretta dei luoghi in cui si sposterà il dispositivo mobile controllato»[41].

Quest'ultimo impegno motivazionale, secondo la riforma dell'art. 267, comma 1, cod. proc. pen. operata dal d.lgs. n. 216 del 2017, non occorre si procede per i delitti di cui all'art. 51, comma 3-*bis* e 3-*quater*, cod. proc. pen.

---

[41] Cfr. Relazione illustrativa al d.lgs. 29 dicembre 2017, n. 216, pag. 10. Secondo G. VARRASO, *Le intercettazioni e i regimi processuali differenziati per i reati di "grande criminalità" e per i delitti dei pubblici ufficiali contro la pubblica amministrazione*, in O. Mazza (a cura di), *Le nuove intercettazioni*, Torino, 2018, 147, la regola della predeterminazione dei luoghi "per ambienti", pur costituendo una garanzia "debole" tenendo conto delle prassi invalse nella motivazione dei provvedimenti autorizzativi delle intercettazioni, sarebbe comunque in grado, se correttamente intesa, in termini di «progetto investigativo», di evitare l'effettuazione di "intercettazioni itineranti".

Quanto ai reati contro la pubblica amministrazione, a seguito dell'interpolazione effettuata nell'art. 267 cod. proc. pen. dall'art. 1, comma 4, lett. b), della legge n. 3 del 2019, sembrano possibili due diverse letture:

– secondo un'interpretazione, di natura letterale, anche nei procedimenti per delitti contro la pubblica amministrazione puniti con la reclusione non inferiore nel massimo a cinque anni, nel caso di impiego del captatore informatico al fine di realizzare intercettazioni tra presenti, sarebbe necessaria l'adozione di un decreto autorizzativo del giudice per le indagini preliminari che contenga l'indicazione delle circostanze di tempo e di luogo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono, oltre alle ragioni per le quali è necessario lo strumento tecnologico in esame per la ricerca della prova[42];

– secondo una diversa interpretazione, che si pone in senso diametralmente opposto rispetto alla precedente, così come avviene per i delitti di cui all'art. 51, comma 3-*bis* e comma 3-*quater*, cod. proc. pen., anche "*se si procede per delitti contro la pubblica amministrazione puniti con la reclusione non inferiore nel massimo a cinque anni*", il decreto autorizzativo dell'impiego del captatore non deve avere il contenuto necessario dapprima indicato[43].

Questa seconda lettura appare preferibile, anche perché in tale direzione si ravvisano indicazioni nei lavori preparatori[44].

---

[42] Così, C. PARODI, *Intercettazioni. Come è (ri)cambiata la disciplina dopo i decreti sicurezza e anticorruzione*, in *www.Ilpenalista.it*, 25 gennaio 2019, secondo cui «Anche in relazione alla captazioni in tema di delitti contro la p.a., pertanto, nel momento in cui il provvedimento di autorizzazione deve per forza di cose essere integrato con il dato cronologico e di localizzazione dell'attività, si deve ritenere che un corretto e puntale rispetto di tali precisazione non possa che avvenire tramite un sistema di attivazione "a uomo presente" e non in conseguenza del semplice inserimento del captatore sul *device*».

[43] Cfr. L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione in tema di intercettazioni con captatore informatico*, in *Dir. pen. cont.*, 24 settembre 2019, il quale invita a superare la mera analisi del dato testuale, rilevando che «non avrebbe però alcun significato l'aggiunta di un espresso riferimento alle fattispecie criminose in danno della pubblica amministrazione, se anche queste restassero sottoposte alla medesima disciplina dei reati "comuni"» ed aggiungendo che «ritenere applicabile ai predetti delitti il regime più stringente dettato per i reati "comuni", sarebbe, anzitutto, contrario allo spirito della riforma del 2019, che intende reprimere con forza il fenomeno corruttivo. Inoltre, ci troveremmo di fronte ad una disciplina priva di coerenza: una volta che il legislatore si è spinto sino a consentire l'intrusione domiciliare con agente spia, anche per i reati contro la pubblica amministrazione, non avrebbe alcun senso fare un passo indietro quando si tratta di incidere sulla parte motivazionale del decreto autorizzativo, realizzando una parificazione soltanto "a metà" con i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater*, cod. proc. pen.»; per la medesima soluzione, L. TESCAROLI, *La legge spazzacorrotti: analisi e problematiche delle novità sostanziali e processuali della legge n. 3 del 2019*, in *Questione Giustizia* 11 settembre 2019; M. TORRE, *Il captatore informatico dopo la legge c.d. "spazza-corrotti"*, in *Dir. Pen. e Processo*, 2019, 5, 648, il quale auspica che "l'infelice formulazione dell'art. 267, comma 1, c.p.p." sia superata mediante una interpretazione "terapeutica" di tipo sistematico che faccia leva sulla ratio della novella, aggiungendo che «ciò non ci esime dal censurare l'atteggiamento del legislatore, colpevole di trascurare i dettagli che, in una materia complessa come quella in esame, spesso fanno la differenza»; G. AMATO, *Ammesso senza limiti il "Cavallo di Troia" nelle investigazioni*, in *Guida al diritto* 2019, 7, 86.

[44] Nel Dossier del Servizio Studi del Senato sull'A.S. n. 955-A, infatti, si legge che «In relazione al nuovo contenuto dell'art. 266 c.p.p., la lett. b) modifica l'art. 267 c.p.p. per derogare – in relazione alle intercettazioni con uso dei citati captatori informatici (*trojan*) nei procedimenti per delitti contro la P.A. puniti con la

Anche in questo caso, comunque, una norma che è entrata in vigore (cioè, l'art. 1, comma 4, della legge n. 3 del 2019) ha modificato una disposizione del codice di rito (l'art. 267 cod. proc. pen.) che è stata riformata da una norma (l'art. 4 del d.lgs. n. 216 del 2017) la cui applicazione, però, è stata differita da leggi successive ai provvedimenti autorizzativi di intercettazioni successivi al 31 dicembre 2019 e poi, dall'art. 1 del d.l. n. 161 del 2019, ai procedimenti penali iscritti dopo il 29 febbraio 2020.

15. Questioni di diritto intertemporale: La tesi secondo cui il captatore informatico è utilizzabile per le indagini relative ai reati dei pubblici ufficiali contro la pubblica amministrazione a far data dal 26 gennaio 2018.

1. Dopo la riforma ad opera della legge n. 3 del 2019, secondo un orientamento, il captatore informatico è utilizzabile per le indagini relative ai reati dei pubblici ufficiali contro la pubblica amministrazione.

L'art. 9 del d.lgs. n. 216 del 2017, come è stato illustrato, ha previsto il differimento dell'efficacia delle "*disposizioni di cui agli articoli 2, 3 4, 5 e 7*" del medesimo decreto legislativo, con esclusione dell'art. 6 che, invece, regola la disciplina delle intercettazioni nei procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione.

L'art. 6 di tale d.lgs., pertanto, è entrato in vigore dal 26 gennaio 2018. Da questa data, quindi, le operazioni di intercettazione per l'accertamento dei reati contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni sono soggette alla disciplina prevista dall'art. 13 d.l. n. 152 del 1991, originariamente dettata per i reati di criminalità organizzata.

L'art. 13 d.l. n. 152 del 1991, come interpretato dalla giurisprudenza di legittimità nella sentenza "Scurato", permette l'uso del captatore per realizzare intercettazioni tra presenti.

L'art. 6, comma 2, del d.lgs. 216 del 2017, in verità, ha previsto una disciplina particolare per l'impiego del captatore informatico nei luoghi domiciliari nelle indagini relative ai reati contro la pubblica amministrazione. Tale disposizione, infatti, ha stabilito che, nel caso di intercettazioni eseguite tramite captatore informatico in uno dei luoghi di cui all'art. 614 cod. pen., è necessario che sia stata raggiunta la prova che in detto luogo è in corso l'attività criminosa. Questa norma, quindi, non ha esteso ai procedimenti relativi ai reati contro la pubblica amministrazione una delle deroghe alla disciplina ordinaria delle intercettazioni previste dall'art. 13 del d.l. n. 152 del 1991 per le captazioni in materia di criminalità organizzata – quella per la quale per le intercettazioni in ambienti domiciliari non occorre che sia in corso l'attività criminosa – determinando una

reclusione non inferiore nel massimo a cinque anni – alla regola generale che prevede che il decreto motivato del GIP debba indicare le circostanze di tempo e di luogo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono».

sorta di *tertium genus* tra la disciplina delle intercettazioni per reati comuni e quelle di criminalità organizzata[45].

L'art. 1, comma 3, della legge n. 3 del 2019, pubblicata sulla Gazzetta ufficiale del 16 gennaio 2019, tuttavia, ha abrogato proprio l'art. 6, comma 2, del d.lgs. n. 216 del 2017. La norma "abrogante" è vigente dal 31 gennaio 2019, non essendo ricompresa tra quelle per le quali l'entrata in vigore è stata differita dall'art. 1, comma 2, della medesima legge.

L'abrogazione della disposizione indicata del d.lgs. n.216 del 2017 ha determinato l'ampliamento dell'area operativa dell'art. 6, comma 1, del d.lgs. 216 del 2017 che ha esteso, ai reati più gravi dei pubblici ufficiali contro la pubblica amministrazione, la disciplina dell'art. 13 del d.l. n. 152 del 1991 e, implicitamente, anche l'uso del captatore informatico per realizzare le intercettazioni tra presenti.

Più precisamente, dall'abrogazione dell'art. 6, comma 2, del d.lgs. n. 216 del 2017 è derivato l'allargamento del raggio d'azione della previsione derogatoria all'art. 266, comma 2, cod. proc. pen. anche alle indagini relative ai reati indicati.

A partire dal 31 gennaio 2019, dunque, epoca di entrata in vigore dell'art. 1, comma 3, della legge n. 3 del 2019, nei procedimenti per reati contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni trova applicazione, in forza del rinvio contenuto nell'art. 6, comma 1, dello stesso d.lgs., l'intera disciplina dell'art. 13 d.l. n. 152 del 1991, ivi compresa la possibilità di effettuare intercettazioni tra presenti presso luoghi di privata dimora mediante captatore informatico, pure se non sussiste un fondato motivo per ritenere che ivi sia in corso l'attività criminosa[46].

2. L'art. 6, comma 1, della legge n. 3 del 2019, in altri termini, ha esteso la disciplina dell'art. 13 d.l. n. 152 del 1991 ai procedimenti relativi ai più gravi reati dei pubblici ufficiali contro la pubblica amministrazione. Tale ultima disposizione è la fonte normativa che legittima l'impiego del captatore nelle indagini relative ai reati più gravi contro la pubblica amministrazione.

---

[45] Cfr., su questa disposizione, tra gli altri, D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Diritto penale contemporaneo* 2018, 1, 228, il quale, a tal proposito, ritiene si tratti di una «disciplina a metà strada tra quella ordinaria e quella speciale per reati di criminalità organizzata e terrorismo».

[46] È stato rilevato che «la disposizione transitoria dell'art. 9 del d.lgs. 216/2017 non contemplava l'art. 6, che, pertanto, è da tempo in vigore. Non solo: con la l. 3/2019, è stato abrogato il comma secondo del citato art. 6 – che limitava le "potenzialità" contenute nel comma 1 – così che oggi la disciplina delle intercettazioni in tema di reati di p.a. è equiparata in tutto a quella in tema di criminalità organizzata e terrorismo. Ne consegue che, in attesa della piena operatività delle disposizioni generali sull'uso del captatore, l'esecuzione di tali forme di captazioni in tema criminalità organizzata, terrorismo e p.a. non potranno che essere valutate e eseguite in conformità alle indicazioni del testo originario degli artt. 266 e 267 c.p.p. sulla base delle indicazioni della S.C. (e in particolare delle Sezioni unite, 1 luglio 2016, n. 26889)», cfr. C. PARODI, *Intercettazioni. Come è (ri)cambiata la disciplina dopo i decreti sicurezza e anticorruzione*, cit. Volendo, si veda anche L. GIORDANO, *Il ricorso al "captatore informatico" nelle indagini per i reati contro la pubblica amministrazione*, in G. Flora, A. Marandola (a cura di), *La nuova disciplina dei delitti di corruzione, Profili penali e processuali*, Pisa, 2019, 90 e ss.

La giurisprudenza delle Sezioni unite, con la sentenza "Scurato", ha affermato che la disciplina dell'art. 13 d.l. n. 152 del 1991 legittima l'impiego del captatore informatico per realizzare intercettazioni tra presenti; dunque, l'art. 6, comma 1, del d.lgs. n. 216 del 2017 ha permesso l'impiego del captatore informatico per le indagini in cui trova applicazione la norma che deroga alla disciplina codicistica delle intercettazioni.

L'art. 6, comma 2, del d.lgs. n. 216 del 2017, inoltre, non escludeva l'impiego del captatore nel caso di intercettazioni eseguite in uno dei luoghi di cui all'art. 614 cod. pen., ma si limitava a pretendere che, in tale caso, fosse raggiunta la prova che in detto luogo fosse in corso l'attività criminosa.

Questa disposizione è stata abrogata dall'art. 1, comma 3, della legge n. 3 del 2019, permettendo anche in questo ambito la piena applicazione della disciplina dell'art. 13 d.l. n. 152 del 1991.

Si può, pertanto, concludere che:

1) a far data dal 26 gennaio 2018, epoca di entrata in vigore dell'art. 6 del d.lgs. n. 216 del 2017, deve ritenersi ammissibile il ricorso al captatore informatico per le intercettazioni tra presenti nelle indagini per i reati dei pubblici ufficiali contro la pubblica amministrazione, in forza del rinvio all'art. 13 d.l. n. 152 del 1991, come interpretato dalla sentenza delle Sezioni unite "Scurato, contenuto nell'art. 6, comma 1, d.lgs. n. 216 del 2017;

2) dal 31 gennaio 2019, epoca di entrata in vigore della legge n. 3 del 2019, è ammissibile l'impiego dello strumento in esame, per i reati indicati, anche in luoghi domiciliari e in carenza della prova che sia in corso l'attività criminosa in forza:

– dell'art. 6, comma 1, del d.lgs. n. 216 del 2017, che dispone l'applicazione delle disposizioni di cui all'art. 13 del d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203 ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni

– dell'art. 1, comma 3, della legge n. 3 del 2019 che, abrogando l'art. 6, comma 2, del d.lgs. n. 216 del 2017, ha permesso l'applicazione a tali procedimenti anche dell'ultima parte dell'art. 13, comma 1, del d.l. n. 152 del 1991, secondo cui "*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*";

– dei principi espressi dalla sentenza Cass. Sez. unite, n. 26889 del 28/04/2016, Scurato, Rv. 266905, che, nei procedimenti soggetti alla disciplina di cui all'art. 13 del d.l. n. 152 del 1991, ha ritenuto ammissibile l'utilizzo del captatore informatico per realizzare intercettazioni tra presenti.

3. La soluzione illustrata non pare posta in discussione dall'art. 1, comma 4, della legge n. 3 del 2019 che ha modificato gli artt. 266 e 267 cod. proc. pen., in alcune parti, a loro volta, modificate dall'art. 4 del d.lgs. n. 216 del 2017 e non ancora applicabili (in forza del differimento dell'efficacia stabilito dall'art. 9 del d.lgs. n. 216 del 2017).

Con riguardo alla modifica dell'art. 266, comma 2-*bis*, cod. proc. pen., va preso atto che si tratta della disposizione che contempla i "*limiti di ammissibilità*" dello strumento in esame, rendendo "*sempre consentita*" l'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile anche per i reati contro la pubblica amministrazione.

Deve rilevarsi, però, che la modifica all'art. 266, comma 2-*bis*, cod. proc. pen. è stata operata da una norma del 2019 che è entrata in vigore all'esito dell'ordinario periodo di *vacatio legis* e che, quindi, è pienamente efficace.

La fonte normativa che ne legittima l'impiego nei procedimenti per tali reati, in ogni caso, ove non si ritenesse ancora applicabile l'art. 266, comma 2-*bis*, cod. proc. pen. in attesa dell'efficacia dell'art. 4 del d.lgs. n. 216 del 2017, è rappresentata dall'art. 13 del d.l. n. 152 del 1991, cui rinvia l'art. 6, comma 1, dello stesso d.lgs. n. 216 del 2017 (che si intitola "*Disposizioni per 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*"). Pur se si ritenesse inefficace la riforma introdotta dalla legge n. 3 del 2019, sostenendo che l'art. 266, comma 2-*bis*, cod. proc. pen. come riformato sia applicabile solo ai decreti autorizzativi emessi dopo il 31 dicembre 2019, non sarebbe preclusa l'ammissibilità di tale strumento informatico nelle indagini, che è ancorata su altra disposizione certamente vigente.

4. In relazione invece alla modifica dell'art. 267 cod. proc. pen., che disciplina i "*presupposti del decreto autorizzativo*", deve rilevarsi che anche questa norma della legge n. 3 del 2019 è entrata in vigore, non essendo stato differita la sua efficacia nel tempo.

Qualora si ritenesse tale riforma inapplicabile perché, anche in questo caso, incide su una disposizione del codice riformata dal d.lgs. n. 216 del 2017 la cui efficacia è stata differita da interventi normativi successivi ai provvedimenti autorizzativi successivi al 31 dicembre 2019 8 ed attualmente ai procedimenti penali iscritti dopo il 29 febbraio 2020 ex art. 1 d.l. n. 161 del 2019), sarebbe comunque possibile il ricorso al captatore informatico anche per le indagini in tema di delitti di pubblici ufficiali contro la pubblica amministrazione in forza del citato art. 6, comma 1, d.lgs. n. 216 del 2017.

Non occorrerebbe rispettare, pertanto, le peculiari garanzie in tema di motivazione "rafforzata" del decreto autorizzativo, cioè senza che sia necessario indicare le ragioni per le quali lo strumento è necessario nonché le circostanze di tempo e di luogo in cui è attivato il microfono.

Del resto, come è stato già illustrato, è stata anche prospettata una diversa lettura dell'art. 267 cod. proc. pen. come riformato dal d.lgs. n. 216 del 2017 e dalla legge n. 3 del 2019, pur apparentemente contrastante con il dato letterale, indicata dai suoi fautori come più conforme alla *ratio* della nuova legge, secondo cui il decreto autorizzativo "rafforzato" nella motivazione, con l'indicazione dei luoghi e dei tempi in relazione ai quali è necessario l'impiego del captatore, non occorra per i procedimenti relativi a reati di pubblici ufficiali contro la pubblica amministrazione, al pari di quanto previsto per i reati di cui all'art. 51, comma 3-*bis* e comma 3-*quater*, cod. proc. pen. Ciò condurrebbe a far ritenere che basti che il decreto autorizzato indichi le ragioni che rendono necessario – neppure assolutamente indispensabile – l'impiego del captatore informatico.

Tale soluzione, in ogni caso, potrebbe non generare alcuna limitazione delle garanzie dei consociati, ove si valorizzasse l'indirizzo accolto dalle Sezioni unite con la sentenza "Scurato", seguita sul punto da pronunce successive della Corte, secondo cui il provvedimento autorizzativo dell'intercettazione per mezzo del sofisticato meccanismo in esame deve assolvere all'onere di motivazione in modo rigoroso, in particolare con riguardo alla dimostrazione della sussistenza di un reato presupposto che rientra nel novero di quelli a cui si riferisce l'art. 13 del d.l. n. 152 del 1991, tra i quali, ex art. 6, comma 1, della legge n. 3 del 2019, anche i reati contro la pubblica amministrazione. La presenza dei presupposti del provvedimento, previsti dall'art. 13 del d.l. n. 152 del 1991, deve essere ancorata a sufficienti, sicuri e obiettivi elementi indiziari, così ribadendosi l'essenziale funzione di garanzia svolta dalla motivazione del decreto autorizzativo delle intercettazioni, che deve realizzare il corretto bilanciamento tra i diritti costituzionali individuali e collettivi in conflitto[47].

16. segue: La tesi secondo cui i risultati delle intercettazioni tramite captatore informatico non sono utilizzabili per le indagini relative ai reati dei pubblici ufficiali contro la pubblica amministrazione.

1. Una diversa impostazione rileva che il captatore informatico per le indagini relative ai reati dei pubblici ufficiali contro la pubblica amministrazione è stato disciplinato per la prima volta dal d.lgs. n. 216 del 2017.

In particolare, l'art. 4 di tale d.lgs., modificando l'art. 266-*bis* cod. proc. pen. che regola i "*limiti di ammissibilità*" delle intercettazioni, ha disposto che l'intercettazione di dialoghi tra presenti possa avvenire anche per mezzo del *trojan*. L'art. 6, comma 2, dello stesso d.lgs. ha previsto che, per i delitti dei pubblici ufficiali contro la pubblica amministrazione, qualora l'intercettazione tramite captatore informatico avviene in luoghi domiciliari, occorre rispettare la condizione di cui all'art. 266, comma 2, cod. proc. pen. per la quale è necessario che sussista un fondato motivo per ritenere che sia in corso l'attività criminosa.

---

[47] Sottendendo verosimilmente la possibilità del ricorso al *trojan* nelle indagini relative ai reati contro la pubblica amministrazione, ha messo in luce la particolare situazione che si è venuta a creare a seguito dell'abrogazione, con effetto immediato, dell'art. 6, comma 2, del d.lgs. n. 216 del 2017 e le modifiche agli artt. 266 e 267 cod. proc. pen. non ancora applicabili, rilevando, con riferimento ai presupposti del provvedimento autorizzativo delle intercettazioni che «paradossalmente, tale sforzo ermeneutico (quello relativo alla indicazione nel provvedimento autorizzativo delle ragioni per le quali è necessario il ricorso al captatore informatico come prescritto dall'art. 267 cod. proc. pen. non ancora efficace, n.d.r.) non è necessario sino all'entrata in vigore delle nuove disposizioni. *De iure condito*, infatti l'avvenuta abrogazione del comma 2 dell'art. 6 del d. lgs. n. 216 del 2017 ad opera della c.d. legge "spazza-corrotti" ha determinato la legittimazione immediata del captatore informatico quando si procede per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione, senza la necessità di rispettare il *surplus* motivazionale richiesto dal nuovo – ma non ancora entrato in vigore – art. 267, comma 1, c.p.p.» (M. TORRE, *Il captatore informatico dopo la legge c.d. "spazza-corrotti"*, cit. 648).

Come è stato illustrato, l'art. 4 del d.lgs. n. 216 del 2017 non è ancora efficace, essendo stato previsto, per effetto di diversi interventi normativi che hanno riguardato l'art. 9 sempre del d.lgs. n. 216 del 2017, il differimento della sua applicazione.

L'art. 6, comma 2, d.lgs. n. 2017, invece, ai sensi dell'art. 9 del medesimo d.lgs., è entrato in vigore all'esito periodo ordinario di *vacatio legis* (quindici giorni dopo la pubblicazione avvenuta in data 11 gennaio 2018).Questa norma – l'unica entrata in vigore di quelle che disciplinano il captatore informatico – è stata abrogata dalla legge n. 3 del 2019.

L'art. 1, comma 4, della legge n. 3 del 2019, poi, ha modificato l'art. 266, comma 2-*bis*, cod. proc. pen., che disciplina i limiti dell'utilizzo del captatore informatico per compiere intercettazioni, estendendone l'impiego ai reati dei pubblici ufficiali contro la pubblica amministrazione.

L'intervento legislativo del 2019 ha riguardato una disposizione, introdotta dal d.lgs. n. 216 del 2017 non ancora efficace (essendone stata differita l'applicazione dall'art. 9 dello stesso d.lgs. e dalle successive modifiche di tale norma).

L'art. 1, comma 4, della legge n. 3 del 2019, in particolare, non ha disciplinato l'intera materia del captatore informatico, essendosi limitata, invece, ad estendere la disciplina dell'art. 266, comma 2-*bis*, cod. proc. pen. ai reati più gravi dei pubblici ufficiali contro la pubblica amministrazione. La modificazione non riguarda il testo originario dell'art. 266 cod. proc. pen., ma il nuovo comma risultante dalle modifiche del d.lgs. n. 216 del 2017, non ancora vigente o, quanto meno, non applicabile. Ne consegue che la disciplina introdotta dalla legge n. 3 del 2019 non può trovare immediata applicazione, perché "subisce" il differimento previsto per le disposizioni del d.lgs. n. 216 del 2017, rispetto alla quale non ha una propria autonomia[48].

Il differimento dell'applicazione del captatore informatico disposto dall'art. 9 del d.lgs. n. 216 del 2017, del resto, avrebbe un preciso fondamento. Esso, invero, sarebbe derivato dalla necessità di porre in essere le modalità di custodia del materiale intercettato, a loro volta previste dalla nuova legge[49], e, dunque, sarebbe legato alla

---

[48] In dottrina, si veda L. FILIPPI, *Riforme attuate, riforme fallite e riforme mancate degli ultimi 30 anni. Le intercettazioni*, in *Arch. pen*. 2019, 3, 41 e ss., secondo cui «la circostanza che ad essi (ai procedimenti per i reati dei pubblici ufficiali contro la pubblica amministrazione) si applichino, in ragione dell'art. 6, comma 1, d.lgs. n. 216 del 2017, le regole dettate dal citato art. 13, non pare idonea a determinare un'estensione *in malam partem* del *dictum* della menzionata pronuncia (la sentenza Scurato)»; S. SIGNORATO, *Intercettazioni di comunicazioni*, in R. ORLANDI, S. SEMINARA, *Una nuova legge contro la corruzione*, Torino, 2019, 255 e ss. secondo cui «essendo stata prorogata l'entrata in vigore della norma contenitore (art. 266 e 267 cod. proc. pen.) risulta automaticamente prorogato anche il (variato) contenuto», mentre l'abrogazione dell'art. 6, comma 2, del d.lgs. n. 216 del 2017 si limita a semplificare presupposti e condizioni per effettuare le intercettazioni di conversazioni o comunicazioni per i reati dei pubblici ufficiali contro la pubblica amministrazione con mezzi diversi dal *trojan*.

[49] In particolare, nella relazione che accompagna il d.lgs. n. 216 del 2017 si legge che «In relazione alle parti della riforma che sono connesse alla nuova modalità di custodia del materiale intercettativo, è stabilito che acquistino efficacia a decorrere dal centottantesimo giorno successivo all'entrata in vigore. Ciò al fine di consentire ai singoli uffici di dettare le opportune indicazioni funzionali a dare attuazione al nuovo articolo 89-*bis* delle disposizioni di attuazione del codice di procedura penale, che affida la direzione e la

particolare forza intrusiva dello strumento in esame e alla necessità di evitare la divulgazione del materiale raccolto.

Nei procedimenti che riguardano reati contro la pubblica amministrazione, pertanto, non si potrebbe ricorrere al captatore informatico per realizzare intercettazioni tra presenti, perché non è ancora applicabile la disposizione che ne ammette l'impiego. I risultati dell'attività di intercettazione realizzata, di conseguenza, sono da ritenersi inutilizzabili, perché raccolti in forza di un mezzo di ricerca della prova non consentito dalla legge. Il d.l. n. 161 del 2019, come si vedrà meglio nel prosieguo, ha differito l'applicabilità dell'art. 4 del d.lgs. n. 216 del 2017 "*ai procedimenti penali iscritti dopo il 29 febbraio 2020*".

2. Tale impostazione sembra ricevere una conferma dall'inapplicabilità delle disposizioni di garanzia con le quali il legislatore del d.lgs. n. 216 del 2017 ha circondato il procedimento autorizzativo del captatore informatico, le quali mirano a salvaguardare il corretto bilanciamento delle esigenze investigative con le prerogative individuali.

L'art. 1, comma 4, lett. b), della legge n. 3 del 2019, in particolare, come è stato illustrato, ha modificato l'art. 267, comma 1, terzo periodo, cod. proc. pen., come, a sua volta, era stato modificato dal d.lgs. n. 216 del 2017. Questa norma è entrata in vigore. Anche in questo caso, però, il legislatore ha inciso su una disposizione (l'art. 267 cod. proc. pen. come modificato dall'art. 4, comma 1, lett. b), del d.lgs. n. 216 del 2017) che non è ancora efficace, con una norma che, pertanto, pur essendo entrata in vigore, non è applicabile.

La norma non ancora efficace – cioè l'art. 267 cod. proc. pen. come modificato dall'art. 4 del d.lgs. n. 216 del 2017 – ha stabilito che il decreto autorizzativo delle intercettazioni debba avere un contenuto tipico, costituito delle ragioni che rendono necessaria tale modalità di intercettazione e, secondo una certa lettura dapprima illustrata, anche dall'indicazione dei luoghi e dei tempi entro cui è consentita la captazione. Questo contenuto del provvedimento – che, per giunta, non è richiesto dalla sentenza Scurato nei limiti in cui tale decisione ha ritenuto legittimo l'uso del captatore nelle indagini di criminalità organizzata – integra i presupposti dell'autorizzazione, dando attuazione ai principi di cui all'art. 14 e 15 Cost. e dall'art. 8 CEDU. In attesa dell'applicabilità di questi presupposti, non può essere legittimamente adottato un provvedimento di intercettazione tramite captatore per i reati contro la pubblica amministrazione.

3. Una riprova dell'attuale inutilizzabilità del captatore informatico nei reati contro la pubblica amministrazione sembra potersi desumere anche dall'inapplicabilità di altre norme che presidiano l'esecuzione delle operazioni di intercettazione compiute con tale mezzo e l'utilizzabilità dei risultati così ottenuti.

---

sorveglianza dell'archivio riservato al procuratore della Repubblica. Questi, in particolare, dovrà impartire le prescrizioni necessarie a necessarie a garantire la tutela del segreto su quanto ivi custodito».

Anche in questo caso si tratta di norme dettate a garanzia del corretto bilanciamento tra le prerogative individuali e le esigenze investigative.

L'art. 4, comma 1, lett. c), d.lgs. n. 216 del 2017, in particolare, ha introdotto il nuovo art. 268, comma 3-*bis*, cod. proc. pen., permettendo per lo svolgimento di tali intercettazioni il ricorso ad ausiliari di polizia giudiziaria. Vero è che la giurisprudenza di legittimità, come è stato illustrato, ammette il ricorso ad ausiliari per le operazioni di intercettazione, ma nel caso del captatore l'autorizzazione normativa al loro utilizzo, allo stato, non è applicabile.

L'art. 4, comma 1, lett. e), del d.lgs. n. 216 del 2017, infine, ha introdotto nell'art. 271 cod. proc. pen. il nuovo divieto di utilizzazione dei risultati delle intercettazioni tramite captatore, stabilendo che "*Non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo*". Anche questa norma, allo stato, non è efficace.

Si tratta di disposizioni che svolgono una funzione di garanzia, previste per bilanciare la notevole capacità intrusiva del mezzo tecnologico in esame. In attesa dell'applicabilità di queste norme, nei procedimenti per reati contro la pubblica amministrazione non sarebbe dunque possibile ricorrere utilmente alle intercettazioni per mezzo di captatore informatico.

4. L'art. 1, comma 3, della legge n. 3 del 2019, ha abrogato l'art. 6, comma 2, del d.lgs. n. 216 del 2017. Come si è visto, si tratta della norma che, in tema di procedimenti per i più gravi reati dei pubblici ufficiali contro la pubblica amministrazione, legittimando implicitamente l'impiego del captatore informatico, stabiliva che, per l'uso in uno dei luoghi di cui all'art. 614 cod. pen., fosse necessaria la prova che in detto luogo fosse in corso l'attività criminosa.

Potrebbe anche ritenersi, sempre seguendo l'impostazione in esame, che la norma abrogata, nel limitare l'impiego del captatore in determinati ambienti, quanto meno implicitamente, abbia reso ammissibile nelle indagini relative ai delitti indicati il ricorso a questo strumento nel periodo della sua vigenza (dal 26 gennaio 2018 al 31 gennaio 2019).

Per effetto dell'abrogazione, tuttavia, non sarebbe più ammissibile l'utilizzo del captatore informatico in dette indagini, essendo venuta meno la sua "base normativa".

L'abrogazione di questa norma, inoltre, comporta la piena estensione ai procedimenti indicati della disciplina di cui all'art. 13 del d.l. n. 152 del 1991, prevista dall'art. 6, comma 1, della stessa legge n. 3 del 2019 e, cioè il regime "semplificato" dei presupposti, i termini di durata più ampi, la deroga alla previsione di cui all'art. 266, comma 2, cod. proc. pen. sulla necessità che, nel caso di intercettazioni tra presenti nei luoghi di cui all'art. 614 cod. pen. sia in corso l'attività criminosa.

Tale abrogazione, però, non varrebbe a permettere l'estensione del captatore informatico ai reati dei pubblici ufficiali contro la pubblica amministrazione, perché tale estensione è disciplinata da altra disposizione, cioè dall'art. 266, comma 2-*bis*, cod. proc. pen., che, come è stato illustrato, non è ancora efficace, come sembra anche emergere dai lavori preparatori, che esplicitamente alludono ad un'abrogazione determinata da una

mera esigenza di "coordinamento normativo" con la nuova disposizione introdotta nell'art. 266, comma 2-*bis*, cod. proc. pen.[50].

In sintesi, in attesa dell'efficacia degli artt. 266 e 267 cod. proc. pen., come modificati dal d.lgs. n. 216 del 2017 e dalla legge n. 3 del 2019, non basterebbe l'abrogazione dell'art. 6, comma 2, del d.lgs. n. 216 del 2017, con il conseguente ampliamento del raggio d'azione dell'art. 6, comma 1, del medesimo d.lgs. (e, dunque, dell'art. 13 del d.l. n. 152 del 1991), a permettere l'uso del captatore nelle indagini per i reati contro la pubblica amministrazione e a rendere utilizzabili i risultati di una simile attività di intercettazione[51].

17. segue: La soluzione accolta dalle Sezioni unite civili.

Le Sezioni unite civili, sentenza n. 741 del 15/01/2020, con riferimento in particolare alle norme applicabili "*ratione temporis*" in tema di intercettazioni mediante captatore per reati contro la pubblica amministrazione, hanno recepito il primo indirizzo illustrato.

In particolare, è stato rilevato che l'art. 6 d.lgs. n. 216 del 2017 – che, come si è visto, ha parzialmente esteso ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni la disciplina delle intercettazioni prevista per i delitti di criminalità organizzata dall'art. 13 del d.l n. 152 del 1991, convertito con modif. in l. n. 203 del 1991 ed integrato con d.l. n. 306 del 1992, conv. con modif. in l. n. 356 del 1992 – è entrato in vigore il 26gennaio 2018, non essendo tale disposizione indicata tra quelle per le quali l'art. 9 del medesimo decreto legislativo ha disposto il differimento della loro entrata in vigore.

La successiva modifica di tale norma, introdotta dall'art. 1, comma 3, della l. n. 3 del 2019 – la quale, abrogando il comma 2 dell'art. 6 del d.lgs. n. 216 cit. ha eliminato la restrizione dell'uso del captatore informatico nei luoghi indicati dall'art. 614 c.p., così consentendo l'intercettazione in tali luoghi anche se non vi è motivo di ritenere che vi si stia svolgendo attività criminosa – è a sua volta entrata in vigore, a differenza di altre

---

[50] Nel Dossier del Servizio Studi del Senato sull'A.S. n. 955-A cit. si legge che «la disposizione (la norma che abroga l'art. 6, comma 2, del d.lgs. n. 216 del 2017 – ha natura di coordinamento con quanto previsto dall'art. 266 c.p.p. come modificato dall'art. 3 del disegno di legge (poi confluito nell'art. 1, comma 3, della legge n. 3 del 2019)».

[51] Nell'ambito delle posizioni che sembrano escludere l'utilizzabilità del captatore informatico nelle indagini per reati contro la pubblica amministrazione, un autore ha rilevato che si è venuto a determinare "un regime intertemporale asimmetrico", in quanto «la legge "anticorruzione", in materia di intercettazioni, si è sostanzialmente sovrapposta, con efficacia istantanea, a una disciplina che, al contrario, non è ancora formalmente entrata in vigore» . In tale condizione, è stato ritenuto "più probabile" che le previsioni di cui all'art. 266, comma 2-*bis*, cod. proc. pen. e 267, comma 1, cod. proc. pen. «vivano in un regime di sospensione e occorra, piuttosto, attendere la formale e definitiva entrata in vigore di tutte le norme concernenti l'impiego del mezzo insidioso, per realizzare, finalmente, un'uniformità di disciplina» (L. CAMALDO, *Le innovazioni introdotte dalla legge anticorruzione*, cit., 18).

disposizioni della medesima legge per le quali il legislatore ha differito l'entrata in vigore all'1/1/2020, il decimoquinto giorno dalla pubblicazione della legge sulla G.U., avvenuta il 16 gennaio 2019.

Secondo questa decisione, «la possibilità di utilizzare il captatore informatico preesiste e prescinde dalla modifica del testo codicistico operata dall'art. 4 del d. lgs. 216 del 2017, e deriva direttamente, come hanno precisato le sezioni unite penali, dall'art. 13 del d.l. 152 del 1991, norma il cui ambito di efficacia è stato esteso dall'art. 6 del d. lgs. 261 del 2017 anche ai più gravi reati contro la p.a.».