3/2017

DOPO LE SEZIONI UNITE SUL "CAPTATORE INFORMATICO": AVANZANO NUOVE QUESTIONI, RITORNA IL TEMA DELLA FUNZIONE DI GARANZIA DEL DECRETO AUTORIZZATIVO(*)

Osservazioni a seguito di Cass., SSUU, sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, ric. Scurato

di Luigi Giordano

Abstract. *La sentenza delle Sezioni unite "Scurato", piuttosto che segnare il definitivo superamento dei problemi interpretativi sull'ammissibilità delle intercettazioni per mezzo del cd. "captatore informatico", impone di affrontare nuove questioni come il pericolo di "strumentalizzazione" del delitto associativo, la difficoltà di qualificare l'uso" che è stato fatto del "trojan nella specifica indagine, il suo impiego per l'acquisizione di e-mail "parcheggiate" nell'account o per la registrazione delle "chat". Esse sottendono un tema fondamentale della disciplina delle intercettazioni: il recupero della funzione di garanzia del decreto che autorizza il mezzo di ricerca della prova.*

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

Poche questioni hanno suscitato un dibattito tanto animato come quella dell'utilizzabilità dei risultati delle intercettazioni compiute tramite un software del tipo

(*) Il contributo costituisce il testo della relazione tenuta dall'Autore al Convegno "*Lo stato dell'arte in tema di intercettazioni telefoniche ed ambientali, tra nuove tecnologie, ritardi del legislatore, giurisprudenza suppletiva ed esigenze di tutela del diritto di difesa*", organizzato dalla Camera penale di Napoli il 16 febbraio 2017.

definito simbolicamente "*trojan horse*"[1]. Sebbene rare siano state le pronunce che si sono confrontate con questo genere di programmi, chiamato anche "captatore informatico" o "agente intrusore"[2], il tema ha attratto l'attenzione degli studiosi che hanno immediatamente percepito le potenzialità del nuovo mezzo tecnologico.

Con la sentenza pronunciata il 28 aprile 2016[3], le Sezioni Unite hanno posto un punto fermo, aprendo all'impiego dello strumento per la realizzazione di intercettazioni "tra presenti"[4] 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,

---

[1] In dottrina hanno affrontato il tema, tra gli altri, ATERNO, *Digital forensics (investigazioni informatiche)*, in *Digesto pen.*, Agg. VIII, Torino, 2014, 217; FLOR, *Lotta alla "criminalità informatica e tutela di tradizionali e nuovi diritti fondamentali nell'era di internet*, in *questa Rivista*, 22 settembre 2012; IOVENE, *Le cd. perquisizioni on line: tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *questa Rivista*, 27 febbraio 2014; LORENZETTO, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico"*, nota a Trib. Palermo, Sez. riesame, ord. 11 gennaio 2016, Pres. est. Gamberini, in *questa Rivista*, 24 marzo 2016; MARCOLINI, *Le cosiddette perquisizioni on line (o perquisizioni elettroniche)*, in *Cass. pen.* 2010, 2855; Id., *Le indagini atipiche a contenuto tecnologico nel processo penale: Una proposta*, in *Cass. pen.* 2015, 760 e ss.; TESTAGUZZA, *I sistemi di controllo remoto: tra normativa e prassi*, in *Dir. pen. proc.* 2014, 759; TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. proc.* 2015, 1163; TROGU, *Le intercettazioni di comunicazioni a mezzo Skype*, in *Proc. pen. giust*. 2014, 102.

[2] I precedenti di legittimità sono rappresentati da Cass. Sez. V, 14 ottobre 2009 n. 16556 (dep. 29 aprile 2010), Virruso, in *CED Cassazione* n. 246954, che ha giudicato legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel "personal computer" in uso all'imputato e installato presso un ufficio pubblico e da Cass. Sez. VI, 26 maggio 2015 n. 27100 (dep. 26 giugno 2015), Musumeci, in *CED Cassazione* n. 265654 che ha giudicato legittimo l'impiego dello strumento solo quando il decreto autorizzativo individui con precisione i luoghi in cui espletare l'attività captativa. Nella giurisprudenza di merito, si segnala un decreto del G.i.p. del Tribunale di Napoli, Sez. IV, adottata nella vicenda denominata dagli organi di stampa "P4" per il quale si rinvia a Testaguzza, *Sistemi di controllo remoto: fra normativa e prassi*, cit. e a TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, cit.

[3] 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, p. 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 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, fasc. 5, 21, con nota di FELICIONI, *L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma*. Sulla sentenza si veda anche GAITO – FÙRFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen*. 2016, II, 309; CISTERNA, *Spazio ed intercettazioni, una liaison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite,* in *Arch. pen*. 2016, II, 331; 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; PICOTTI, *Spunti di riflessione per il penalista dalla sentenza delle Sezioni unite relativa alle intercettazioni mediante captatore informatico*, in *Arch. pen*. 2016, II, 354; LASAGNI, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, in *questa Rivista*, 7 ottobre 2016.

[4] Le Sezioni unite hanno precisato che l'espressione "intercettazioni ambientali" è invalsa nella prassi in un'epoca in cui detto genere di captazioni necessitava dell'apposizione di un mezzo tecnologico in un preciso ambiente, mentre il codice di rito, con maggiore precisione, utilizza la locuzione intercettazioni "tra presenti", a riprova che la determinazione del luogo in cui avvengono le rilevazioni non è un presupposto di legittimità del provvedimento.

comma 2, cod. proc. pen., consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto[5]. Al contrario, è stato escluso l'utilizzo del mezzo per reati diversi perché, non essendo possibile prevedere i luoghi di privata dimora nei quali il dispositivo elettronico potrebbe essere introdotto, non si può verificare il rispetto della condizione di legittimità richiesta dall'art. 266, comma 2, cod. proc. pen.

Lungi dal segnare la definitiva soluzione di ogni problema interpretativo sull'ammissibilità dell'uso del mezzo tecnologico nelle indagini, questa decisione stimola nuove riflessioni e impone di affrontare nuove questioni.

2. La necessità del nuovo strumento per lo svolgimento delle indagini.

Le Sezioni unite hanno cercato un punto di equilibrio tra gli interessi contrapposti, fissando i limiti necessari per garantire un impiego del nuovo mezzo compatibile con il rispetto dei diritti individuali.

Una chiusura non sarebbe stata proponibile perché avrebbe significato non comprendere che i nuovi strumenti di comunicazioni sono a disposizione di chiunque. È ormai comune l'uso della messaggistica su computer o su smartphone (chat, audio, video); tutti usiamo *Whatsapp*, che ha soppiantato in breve tempo gli SMS, i quali, peraltro, resistono potendo contare su una nicchia di "affezionati"; per molti è usuale servirsi per le chiamate vocali o quelle video di sistemi *Voip* e non del normale telefono[6].

È diffuso, per esempio, l'impiego di *Snapchat*. Si tratta di un'applicazione che permette di scambiarsi foto e brevi video che vengono cancellati automaticamente al termine della visualizzazione. Permette inoltre di "chattare" in tempo reale e di condividere album pubblici di foto e video accessibili da tutti i propri contatti per un periodo di 24 ore.

È analogamente comune l'utilizzo di *Telegram*, un servizio di messaggistica istantanea basato su *cloud*. Alle conversazioni (*chat*) classiche che rimangono in chiaro sui server della società che eroga il servizio, è stata aggiunta la cifratura *end-to-end* (cioè punto-punto), ossia fra i due dispositivi coinvolti nella conversazione e non sui server.

L'indirizzo, ormai inarrestabile, infatti, è verso l'impiego nelle comunicazioni informatiche di sistemi di cifratura evoluti per aumentare la *privacy*. Tutti abbiamo ricevuto il messaggio di *Whatsapp*: "*I messaggi che invii in questa chat e le chiamate sono ora*

---

[5] La questione proposta alle Sezioni Unite, sollevata dalla Sesta Sezione con ordinanza del 10 marzo 2016, n. 13884, è stata così sintetizzata nella sentenza: «Se – anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa – sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portati (ad es., personal computer, *tablet*, *smartphone*, ecc.)».

[6] Il *trojan* 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* da CAJANI, *Odissea del captatore informatico*, in *Cass. pen.* 2016, 4143.

protetti con la crittografia end-to-end. Tocca per maggiori informazioni". Questa informazione segna un ulteriore passo in avanti: la sicurezza della conversazione si sposta dall'inviolabilità del *server* a quella del dispositivo "servito"; la chiave di cifratura è nota solo agli interlocutori, cioè agli apparecchi in contatto; il *server* non archivia e non legge i messaggi (o, quanto meno, dichiara di non farlo).

A questo punto, come si intuisce, l'uso del captatore è indispensabile nel corso delle indagini per carpire una parte quantitativamente rilevante delle comunicazioni tra le persone che, senza penetrare il dispositivo di uno degli interlocutori, sfuggirebbero ad ogni possibilità di ascolto, persino con la collaborazione delle imprese che erogano i servizi.

Anche i mezzi tecnologici usati nelle inchieste, di conseguenza, debbono evolversi. Pensare che l'attività investigativa debba essere tenuta fuori da queste tecnologie è semplicemente anacronistico, oltre che oltremodo pericoloso perché limita l'efficacia delle inchieste giudiziarie.

Non bisogna pensare che l'impiego dello strumento informatico sia facile.

Dal punto di vista tecnico vanno affrontati una serie di problemi (per esempio, l'eccessivo uso delle batterie dei dispositivi portatili, la necessità di sfuggire agli antivirus e ai *firewall*). Bisogna superare, in particolare, i limiti che i tecnici hardware hanno impostato sul dispositivo 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 questo è possibile "da remoto" e, dunque senza accedere materialmente al dispositivo.

Tutto ciò, come è comprensibile, comporta un costo ingente, che necessariamente fa aumentare la spesa necessaria per compiere indagini[7].

3. La funzione di garanzia del decreto di autorizzazione delle intercettazioni.

Sebbene limiti l'impiego del nuovo mezzo tecnologico ai soli reati più gravi, la decisione delle Sezioni unite ha provocato critiche, anche decise. Tra esse merita di essere segnalata la "*Denuncia dei rischi connessi all'installazione occulta di virus informatici su smartphone e tablet per finalità di indagine penale*", formulata da alcuni docenti dell'Università di Torino con la quale, traendo spunto dalla preoccupazione ingenerata dalla affermata legittimità, sia pure a determinate condizioni, del mezzo di ricerca della prova, si è auspicato l'intervento del legislatore con specifiche disposizioni volte a regolare la materia, realizzando un adeguato bilanciamento dei principi costituzionali e convenzionali coinvolti[8].

[7] Il tema dei costi, in particolare per l'aggiornamento dei programmi di intrusione, è sottolineato, tra gli altri, da MILOSA, *Sos antiterrorismo: "WhatsApp sfugge alle intercettazioni"*, in *Il Fatto quotidiano*, 13 ottobre 2016.

[8] La denuncia è reperibile in rete nel sito istituzionale dell'Università di Torino.

Diversamente[9], è stato rivolto un invito a distinguere l'uso di tale tecnica per effettuare intercettazioni ambientali dal suo impiego per perquisire a distanza gli archivi di computer, *tablet*, *smartphone*. Sotto quest'ultimo aspetto è stato affermato che «l'ipotesi fuoriesce addirittura dal raggio d'azione degli art. 14 e 15 Cost.» e, dunque, non basterebbe una disciplina normativa, ma sarebbe necessario l'affermazione di un nuovo (ed inedito) diritto fondamentale all'uso libero e riservato delle tecnologie informatiche. Non consistendo in una intrusione fisica in una privata dimora, infatti, le perquisizioni *on-line* non minacciano il domicilio. Frugare fra i file contenuti in un *hard disk*, inoltre, è attività diversa dal carpire il flusso di una corrispondenza o di un dialogo in atto, che non lede la libertà e la segretezza delle comunicazioni. In questa prospettiva, è stata indicata a modello l'elaborazione della Corte costituzionale tedesca che, in una nota sentenza del febbraio 2008, ha affermato un apposito diritto fondamentale ("*il diritto all'uso riservato e confidenziale delle tecnologie informatiche*"), derivato dalla dignità della persona, matrice dei diritti fondamentali[10].

In relazione al primo profilo, cioè all'uso del captatore per compire intercettazioni, invece, in presenza della base legale individuata dalla Suprema Corte, non si pone la necessità di un intervento del legislatore. Semmai si avverte il rischio di abusi investigativi per mezzo del grimaldello della "criminalità organizzata"[11].

Di questo pericolo, invero, sono perfettamente consapevoli le Sezioni unite.

Riconoscendo la forza intrusiva del mezzo usato sulle prerogative individuali, la Corte ha precisato che «la qualificazione del fatto reato, ricompreso nella nozione di

---

[9] ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, in *Archivio pen. (web)*, 25 luglio 2016.

[10] Si tratta della sentenza del *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 *questa Rivista*, 8 maggio 2016, sulla quale sia consentito il rinvio a GIORDANO-VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*), con la quale è stato ribadito che, anche nel caso di investigazioni compiute per mezzo di strumenti tecnologici che garantiscono l'accesso da remoto ai sistemi informatici, va garantito il nucleo della vita privata ("*Kernbereich privater Lebensgestaltung*" nella versione originale tedesca, "*core area of private life*", nella traduzione inglese del comunicato stampa della Corte), non tutelato adeguatamente, secondo la Corte, dal paragrafo 20k della legge federale denominata "*Bundeskriminalamtgesetz*" – BKAG – che disciplina i compiti e l'attività della forza di polizia federale, la quale prevede il controllo dei dati raccolti ad opera del personale dell'ufficio federale di polizia penale e non di soggetti esterni e indipendenti. Al riguardo, infatti, va segnalato che la disciplina delle intercettazioni in Germania è caratterizzata dall'intangibilità assoluta del nucleo caratterizzante la vita privata e dal controllo politico-parlamentare (cfr. RUGGERI, *Le intercettazioni e la sorveglianza di comunicazioni e dati nei Paesi di area tedesca*, in AA.VV., *Le intercettazioni di conversazioni, Un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti, Atti del Convegno dell'Associazione tra gli studiosi della procedura penale*, Milano, 2007, 218).

[11] ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di procedura penale sul problema dei captatori informatici*, cit.

criminalità organizzata, deve risultare ancorata a sufficienti, sicuri e obiettivi elementi indiziari, evidenziati nella motivazione del provvedimento di autorizzazione in modo rigoroso».

In questa prospettiva ritorna un tema fondamentale: la necessità di recuperare la funzione di garanzia del decreto che autorizza le intercettazioni.

L'impiego del mezzo altamente tecnologico, infatti, non muta il problema principale della disciplina delle intercettazioni. Il bilanciamento tra i diritti costituzionali confliggenti, individuali e collettivi, deve intervenire nella motivazione del provvedimento autorizzativo[12].

Pur dovendo essere sobria e, dunque, potendo consistere in quella "*minima necessaria a chiarire le ragioni del provvedimento*"[13], la motivazione del decreto 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[14]. Come ha suggerito da tempo la Suprema Corte[15], il giudice deve dare conto della ragione dell'intrusione nella sfera della libertà di comunicare di una determinata

---

[12] Secondo Cass. pen, Sez. VI, 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».

[13] Cfr., tra le altre, Cass. pen., Sez. V, 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. VI, 22 dicembre 1998, n. 4057, in *Cass. pen.* 2000, 3353).

[14] 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. II, 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. VI, 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. NAPPI, *Sull'abuso delle intercettazioni,* in *Cass. pen.* 2009, 471).

[15] Cass. pen., Sez. VI, 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 (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"*.

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. Questo è l'aspetto più denso di significato dell'obbligo di motivazione di cui agli artt. 15 Cost. e 267, co. 1, c.p.p. Il G.i.p., insomma, ha *"l'obbligo di spiegare il perché di un'intercettazione"*[16].

In questa direzione è determinante la crescita della professionalità del pubblico ministero e, soprattutto, del giudicante: quest'ultimo, da un lato, deve avere ben chiaro che l'autorizzazione di un'intercettazione non gli impone di formulare una prognosi di colpevolezza, pena l'espunzione del mezzo di ricerca della prova dagli strumenti investigativi a disposizione del pubblico ministero; dall'altro, deve compiere un vaglio approfondito sulla particolare serietà delle esigenze investigative, cogliendo il collegamento tra la persona le cui conversazioni sono captate e la specifica ipotesi delittuosa oggetto di investigazione. A tale proposito, l'esperienza del giudicante è una condizione necessaria.

4. Il pericolo di strumentalizzazione del reato associativo.

Il bilanciamento tra i diritti contrapposti compiuto dalle Sezioni unite, consentendo l'uso del *trojan* per i soli reati di criminalità organizzata, invero, potrebbe cedere sotto l'effetto congiunto di due colpi.

Come ha segnalato l'autorevole dottrina citata, potrebbero aumentare le intercettazioni fondate su ipotesi di reati associativi, configurati come una sorta di illecito "contenitore", magari senza una specifica individuazione dei delitti scopo dell'associazione ipotizzata. Si tratta di un problema noto e stigmatizzato da tempo[17], che potrebbe accentuarsi perché, senza una configurazione associativa del reato per il quale si svolgono le indagini, non potrebbe essere utilizzato lo strumento informatico in esame.

A questo va aggiunto che la scelta di impiegare un reato di criminalità organizzata come "grimaldello" potrebbe ricevere un avallo indiretto dall'indirizzo giurisprudenziale che sterilizza le conseguenze della diversa qualificazione giuridica del fatto per il quale è stata disposta la captazione. I risultati delle intercettazioni telefoniche disposte per un reato rientrante tra quelli indicati nell'art. 266 cod. proc. pen. sono utilizzabili anche relativamente ad altri reati per i quali si procede nel medesimo procedimento, pur se per essi le intercettazioni non sarebbero state consentite[18].

---

[16] L'espressione è tratta da GREVI, *L'obbligo di spiegare il "perché" di una intercettazione*, in *Corriere della Sera* 14 aprile 2009.

[17] Cfr. NAPPI, *Sull'abuso*, cit., p. 471, secondo cui *"… vengono ammesse intercettazioni con riferimento ad evanescenti ipotesi di reati associativi. E anche quando l'evento del reato è ben individuato, come ad esempio un omicidio, può accedere che non risulti proposta la descrizione di un contesto criminale idoneo a giustificare quella determinata richiesta di intercettazione"*.

[18] Cass. Sez. F, 23 agosto 2016 n. 35536 (dep. 26 agosto 2016), in *CED Cassazione* n. 267598. Secondo Cass., Sez. V, 16 marzo 2016, n. 45535 (dep. 28 ottobre 2016) in *CED Cassazione* n. Rv. 268453, l'utilizzabilità presuppone che tra il contenuto dell'originaria notizia di reato alla base dell'autorizzazione e quello dei reati

Sussiste, in altri termini, il rischio di una strumentalizzazione della qualificazione giuridica associativa nel corso delle investigazioni al fine di ottenere l'autorizzazione di intercettazioni per mezzo del captatore informatico che potrebbero essere utilizzate a fini di prova per reati diversi per i quali non sarebbe stato ammesso l'impiego dello strumento[19].

Per scongiurare questo pericolo, però, ancora una volta non si può che confidare nella professionalità del pubblico ministero[20] e del giudice delle indagini preliminari. Quest'ultimo, in particolare, non deve vanificare il richiamo al rigore della motivazione proveniente dalla Corte di cassazione, verificando con puntualità i presupposti per l'adozione del provvedimento. L'alternativa potrebbe essere solo la strada più semplice dell'aprioristica resistenza all'impiego del mezzo investigativo in esame. Lungi dal determinare un aumento delle garanzie individuali, costituirebbe solo una fuga dal difficile compito assegnato al giudice nella società moderna di bilanciare i diritti costituzionali confliggenti.

Alla Suprema Corte, invece, potrebbe essere richiesta una puntualizzazione sull'area operativa dell'indirizzo dapprima descritto, di cui, peraltro, si colgono i prodromi[21].

5. La principale obiezione alla soluzione delle Sezioni unite. La scelta profonda della sentenza Scurato.

La delimitazione dell'impiego del captatore per i soli reati di criminalità organizzata discende dalle caratteristiche tecniche del mezzo elettronico utilizzato come moderna microspia. Trattandosi di uno strumento "itinerante", prima o poi, finisce con registrare colloqui all'interno di un domicilio. È per questa ragione che il captatore è

---

per cui si procede separatamente vi sia una stretta connessione sotto il profilo oggettivo, probatorio o finalistico, cosicché il relativo procedimento possa ritenersi non diverso rispetto al primo, ai sensi dell'art. 270, comma 1, cod. proc. pen.

[19] Il tema, in particolare, è stato segnalato da VERDE, *Le inchieste di Napoli e le intercettazioni "esplorative"*, in *Il Mattino*, 13 gennaio 2017.

[20] È stato segnalato (CAJANI, *Odissea del captatore informatico*, cit. 4151) il rilievo, ai fini del rispetto dei diritti fondamentali delle persone interessate, dell'attività del pubblico ministero. Egli, nella richiesta di intercettazione, deve descrivere puntualmente al G.i.p. l'operatività del software e le funzioni che si intende attivare; nella fase esecutiva, deve disporre la precisa verbalizzazione delle operazioni con le quali è avvenuta l'installazione del *trojan*; infine, deve procedere al sequestro del dispositivo alla fine delle operazioni allo scopo di garantire il successivo contraddittorio in un futuro dibattimento sulle modalità di raccolta delle prove.

[21] In particolare, a fronte dell'indirizzo prevalente che "sterilizza" le conseguenze della diversa qualificazione del fatto per il quale sono state disposte le intercettazioni, vi è un orientamento che è contrario all'impiego delle captazioni per reati per i quali non sussistono i presupposti di ammissibilità dell'istituto. Si veda Cass., Sez. II, 18 dicembre 2015 n. 1924 (dep. 19 gennaio 2016), in *CED Cassazione* n. 265989; Cass., Sez. III, 25 febbraio 2010 n. 12562 (dep. 31 marzo 2010), in *CED Cassazione* n. 246594; Cass., Sez. VI, 15 gennaio 2004, n. 4942 (dep. 6 febbraio 2004), in *CED Cassazione* n. 229999

stato riservato dalla Suprema Corte ai soli casi in cui la normativa speciale permette di derogare alla tutela del domicilio.

Su questo punto, però, sono state sollevate notevoli riserve[22].

Ad esempio, è stato ipotizzato che l'autorizzazione del giudice potrebbe essere circoscritta alle conversazioni che avverranno in un determinato luogo pubblico o aperto al pubblico. Il dispositivo infettato, inoltre, potrebbe essere un personal computer installato in un determinato posto non domiciliare e non trasportabile ovvero in un portatile abitualmente tenuto fermo[23]. Ma soprattutto l'agente intrusore è controllabile a distanza; il microfono può essere acceso o spento a richiesta e lo smartphone può essere "tracciato", così evitando di procedere a registrazioni quando il portatore del telefono infettato entra in un domicilio; anzi è necessario spegnere il microfono per evitare abnormi consumi della batteria del cellullare che potrebbero insospettire la persona intercettata[24].

Le critiche illustrate evidenzierebbero i limiti strutturali della decisione delle Sezioni unite, che non avrebbe tenuto in debito conto questi profili[25].

Proprio queste obiezioni, al contrario, permettono di cogliere la scelta più profonda della sentenza Scurato.

La Corte, in considerazione della profonda invasività del mezzo e dei rischi per la libertà di comunicare anche degli eventuali terzi, non ha voluto legittimare l'adozione di un'autorizzazione di intercettazioni "al buio", cioè concessa senza poter valutare preventivamente lo svolgimento di attività criminosa nel luogo domiciliare in cui potrebbe essere introdotto il dispositivo. Nella sentenza 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

---

[22] Si veda al riguardo CAMON, *Cavalli di troia*, cit., 93.

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

[24] 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.

[25] 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).
Dopo la sentenza "Scurato", l'eccezione di inutilizzabilità delle intercettazioni compiute per mezzo del software è stata formulata in un giudizio avente ad oggetto reati di corruzione, falso, turbativa d'asta, truffa ed altro (Cass., Sez. V, 4 marzo 2016, n. 26817, in *CED Cassazione* n. 267889). In questo caso, la Corte, pur dando atto in motivazione dell'intervenuto pronunciamento delle Sezioni unite, ha rigettato l'eccezione ribadendo l'orientamento consolidato secondo cui è onere della parte che lamenti l'inutilizzabilità dei risultati delle intercettazioni indicare con precisione l'atto asseritamente affetto dal vizio denunciato e curare e che lo stesso sia acquisito al fascicolo trasmesso al giudice di legittimità, anche provvedendo a produrlo in copia nel giudizio di cassazione (cfr. Cass. Sez. II, 11 aprile 2013, n. 24925, in *CED Cassazione* n. 256540).

dell'autorizzazione…». Si è voluto evitare alla radice il rischio di realizzare intercettazioni tra presenti in luoghi di privata dimora.

In questa prospettiva, in particolare, le Sezioni unite hanno reputato **insoddisfacente la tutela "postuma" delle prerogative individuali che potrebbe derivare dall'applicazione della sanzione dell'inutilizzabilità che colpirebbe le sole intercettazioni eventualmente avvenute in luoghi di privata dimora** al di fuori dei presupposti di cui all'art. 266, comma 2, cod. proc. pen.: l'inutilizzabilità, infatti, va 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[26].

6. La nozione di criminalità organizzata.

Dal momento in cui è stato reputato legittimo l'impiego del virus auto-installante per la realizzazione di intercettazioni "tra presenti" limitatamente ai delitti di "criminalità organizzata"[27], il tema si sposta. Fornire la nozione di "criminalità organizzata" non costituisce un mero esercizio teorico, perché da essa dipende l'applicazione delle norme processuali che si riferiscono specificamente a detta categoria di reati, tra le quali proprio il citato art. 13 del decreto legge n. 152 del 1991.

Su questo punto, la Corte ha ribadito la validità dell'approccio "teleologico" o "finalistico", secondo il quale il significato dell'espressione "criminalità organizzata" deve essere definito avendo riguardo alle finalità specifiche della singola disciplina che deroga alle regole processuali generali. È stata avallata **una nozione ampia di "delitti di criminalità organizzata", che valorizza le finalità perseguite dalla norma**, le quali mirano a riconoscere uno strumento efficace di repressione di reati più gravi[28]. Sono

[26] 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. VI, 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).

[27] Secondo la decisione, per questo genere di reati, l'installazione del captatore informatico in un dispositivo "itinerante" costituisce «una delle naturali modalità di attuazione delle intercettazioni», al pari della collocazione di microspie all'interno di un luogo di privata dimora. Escludendo espressamente il requisito autorizzativo previsto dall'art. 266, comma 2, secondo periodo, cod. proc. pen. il legislatore «ha operato evidentemente uno specifico bilanciamento di interessi, optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio tenendo conto dell'eccezionale gravità e pericolosità, per l'intera collettività, dei (particolari) reati oggetto di attività investigativa per l'acquisizione delle prove».

[28] La sentenza ha ritenuto di dover confermare la validità di questo indirizzo giurisprudenziale, «perché consente di cogliere l'essenza del delitto di criminalità organizzata e nel contempo di ricomprendere tutti i suoi molteplici aspetti, nell'ottica riconducibile alla ratio che ha ispirato gli interventi del legislatore in materia, tesi a contrastare nel modo più efficace quei reati che per la struttura organizzativa che presuppongono e per le finalità perseguite – costituiscono fenomeni di elevata pericolosità sociale».

ricomprese in detta categoria, pertanto, attività criminose eterogenee, purché realizzate da una pluralità di soggetti, i quali, per la commissione del reato, abbiano costituito un apposito apparato organizzativo, con esclusione del mero concorso di persone nel reato. Ad essa non sono riconducibili solo i reati di criminalità mafiosa, ma tutte le fattispecie criminose di tipo associativo. È sufficiente la costituzione di un apparato organizzativo, la cui struttura assume un ruolo preminente rispetto ai singoli partecipanti.

Esula dall'area dei delitti di criminalità organizzata il mero concorso di persone nel reato, pur se caratterizzato da un'attività di organizzazione di risorse materiali ed umane, con rilievo predominante rispetto all'apporto dei singoli concorrenti.

Al riguardo, l'aspetto più delicato non appare quello del riferimento ai delitti di terrorismo[29], quanto la difficoltà di tracciare un confine sufficientemente delineato tra la fattispecie associativa e il concorso di persone nel corso delle indagini[30]. Su questa delimitazione si fonda la funzione di garanzia del decreto di autorizzazione. Eppure essa, secondo l'indirizzo prevalente in giurisprudenza, si fonda sul tasso di precisione dell'accordo criminoso[31].

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

Non sempre, però, è agevole comprendere quale uso del mezzo tecnologico sia stato fatto nella specifica indagine e, dunque, procedere alla relativa qualificazione giuridica.

La vicenda trattata da una recente decisione della Suprema Corte permette di cogliere la portata del problema[32].

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[33]. Le e-mail, in particolare, sono state oggetto di un provvedimento

---

[29] Secondo TESTAGUZZA, *Exitus acta probat "Trojan di Stato": La composizione di un conflitto*, in *Arch. pen.* 2016, 2, in particolare, al fine di delimitare l'ambito di operatività del mezzo tecnologico in esame, «il riferimento ai delitti con finalità di terrorismo … impone una connotazione in via "principale" degli stessi e non anche "accessoria" o meramente "qualificante" come sostenuto dal Supremo consesso».

[30] Cfr. CAMON, *Cavalli di troia in Cassazione*, cit., pag. 93.

[31] Cfr., tra le altre, Cass., Sez. II, 4 ottobre 2016, n. 53000 (dep. 14 dicembre 2016), in *CED Cassazione* n. 268540 Cass., Sez. 4, 16 ottobre 2013 n. 51716 (dep. 23 dicembre 2013), in *CED Cassazione* n. 257906; Cass., Sez. II, 11 ottobre 2013, n. 933 (dep. 13 gennaio 2014), in *CED Cassazione* n. 258009.

[32] Cass., Sez. IV, 28 giugno 2016, n. 40903, in *CED Cassazione* n. 268228.

[33] 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

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».

Su questo punto appare legittimo dissentire.

Non sembra, 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[34]. Appare arduo ricomprendere la digitazione sulla tastiera 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.

---

informazioni più riservate, come quelle che avevano ad oggetto i numeri telefonici "dedicati" allo svolgimento delle singole operazioni di importazione di droga.

[34] Nel caso di specie, dunque, l'acquisizione del flusso informativo non è avvenuto mediante la duplicazione della casella di posta elettronica da parte del gestore, con il conseguente inoltro di tutte le e-mail al server della Procura della Repubblica, ma penetrando all'interno della casella di posta elettronica grazie all'acquisizione delle credenziali. In questo modo, sono state carpite mail in un *account* di posta elettronica *@hotmail.com* gestita da una società statunitense, il cui server è allocato in territorio americano e che, verosimilmente, avrebbe potuto porre ostacoli agli investigatori. Sull'acquisizione delle e-mail si veda MANCUSO, *L'acquisizione di contenuti e-mail*, in Scalfati (a cura di), *Le indagini atipiche*, Torino, 2014, 53.

8. La captazione delle e-mail "parcheggiate", di quelle "bozza" e delle "*chat*" non contestualmente al loro svilupparsi.

La stessa decisione appena illustrata induce a riflettere su un'ulteriore implicazione dell'apertura all'uso del *trojan* nel corso delle indagini. Questo strumento, come si è visto, ha reso agevole di carpire il contenuto delle e-mail pervenute o inviate al destinatario e archiviate nelle cartelle della posta elettronica[35]. Appare ipotizzabile che analogo sia l'effetto sulle "*chat*" il cui contenuto potrebbe essere appreso anche non contestualmente al loro svilupparsi.

Secondo la decisione illustrata, in altri termini, perché sia integrata un'intercettazione, non è necessaria l'attualità della comunicazione rispetto all'atto acquisitivo, essendo sufficiente che ricorra il dato storico dell'inoltro del messaggio, anche se precedente al decreto autorizzativo.

Sul punto, la sentenza illustrata ha seguito un indirizzo giurisprudenziale che sembra sorto con riferimento alle "*chat*" di *Blackberry*. È stata ritenuta legittima l'acquisizione di contenuti di tali messaggi mediante intercettazione operata ai sensi dell'art. 266 cod. proc. pen. poiché le conversazioni, anche se non contestuali, costituiscono un flusso di comunicazioni[36].

Il superamento del presupposto della necessaria captazione in tempo reale rispetto alla comunicazione, tuttavia, conduce a ritenere legittima anche un'intercettazione che opera "per il passato": il provvedimento adottato in una certa data consentirebbe di acquisire pure le comunicazioni avvenute in precedenza. **Quest'azione non sembra rispettare la tipicità delle intercettazioni**, mezzo di ricerca della prova per definizione rivolto "al futuro", in un sistema processuale che prevede altri strumenti tipici, come i sequestri, che sono circondati da specifiche garanzie, che consistono in atti "a sorpresa", ma che non possono essere compiuti in modo occulto[37].

Queste perplessità, in verità, sembrano trasparire anche dalla stessa sentenza che, su questo specifico punto, contiene una motivazione subordinata, richiamando il provvedimento di sequestro, pure intervenuto nel caso di specie, in funzione di garanzia delle prerogative individuali[38].

---

[35] L'importanza del mezzo tecnologico in esame per l'intercettazione delle caselle di posta elettronica *@.com* è stata illustrata da CAJANI, *Odissea del captatore informatico*, cit. 4145.

[36] Cfr. Cass., Sez. III, 10 novembre 2015, n. 50452 (dep. 23 dicembre 2015), in *CED Cassazione* n. 265615; Cass., Sez. IV, 8 aprile 2016, n. 16670 (dep. 21 aprile 2016), in *CED Cassazione* n. 266983.

[37] Nella situazione descritta, in verità, si pone per gli investigatori un problema di tempestività dell'intervento perché una e-mail "parcheggiata" nell'*account* deve essere acquisita rapidamente perché può essere cancellata in qualsiasi momento dall'utilizzatore. Questa esigenza pratica, verosimilmente, induce a ricondurre l'acquisizione delle e-mail "passate" all'istituto delle intercettazioni informatiche piuttosto che alla disciplina del sequestro.

[38] Nella sentenza, infatti, è precisato che «In ogni caso c'era stato un decreto autorizzativo del Gip che, anche a voler ritenere che quelle già spedite e/o ricevute fossero sequestrabili e non intercettabili, "copriva" in termini di garanzie anche tale acquisizione».

Il sequestro, inoltre, secondo la decisione in esame, giustifica nel procedimento in esame l'acquisizione delle e-mail "bozza"[39]. Sul punto, la sentenza critica la tesi che, per salvaguardare il profilo della contestualità della captazione rispetto alla trasmissione, ravvisa un flusso informatico intercettabile quando, per accedere alla "bozza", si entra nella casella di posta elettronica[40]. La decisione, invece, accoglie il "criterio dell'inoltro": l'invio del messaggio – e non la contestualità della captazione rispetto alla conversazione da parte del mittente al destinatario segnerebbe il discrimine tra l'applicazione della disciplina delle intercettazioni e di quella del sequestro[41].

Anche questo profilo non sembra condivisibile.

Nella decisione, infatti, nonostante la mancata spedizione della e-mail, è descritto un sostanziale "inoltro" di comunicazioni. La condotta degli interessati è così descritta: «Chi accedeva per primo all'account di posta elettronica scriveva un'e-mail e poi, senza spedirla, la "parcheggiava" nella casella bozze. A seguire chi si collegava al medesimo account, andava nella casella bozze, leggeva quanto scritto e poi, con il medesimo sistema, scriveva la risposta e, senza spedirla, la salvava nella casella bozze». Viene rappresentato, in tal modo, uno scambio informativo, un dialogo tra due o più soggetti, che, essendo compiuto mediante accesso ad internet, generava un flusso dati da ritenersi intercettabile ex art. 266-*bis* cod. proc. pen.

9. Le principali iniziative legislative in materia di captatore informatico.

La complessità delle questioni ancora in campo suggerisce da ultimo di soffermarsi sulle principali iniziative legislative che mirano a introdurre una disciplina dell'utilizzo nelle indagini penali del captatore informatico. Anche nella sentenza "Scurato", del resto, sono sinteticamente illustrate le principali proposte per

[39] Secondo la sentenza in esame, in particolare, una "bozza" non è assimilabile ad una corrispondenza, perché il messaggio, essendo appunto una mera "bozza", non è stato spedito al destinatario. La sua detenzione, inoltre, è dell'utente e non del gestore del servizio informatico. L'utente, infatti, è l'unico abilitato all'accesso all'*account* per mezzo delle sue credenziali personali. Questo profilo è stato valorizzato per escludere la necessità di disporre una rogatoria internazionale per eseguire il sequestro dei dati che, seppur allocati in un server straniero, sono detenuti dal titolare delle credenziali e non dalla società che gestisce il servizio. Sul punto, proprio con riferimento alla sentenza in esame, si veda DE NOZZA, *E-mail parcheggiate all'estero, similitudine con il cloud computing: La parola della Cassazione*, in *Sic. e giust*. 2016, 4, 51.

[40] Sia consentito, sul punto, il rinvio a GIORDANO, *Percorsi della giurisprudenza in tema di intercettazioni*, in *Gli Orientamenti delle sezioni penali* 2015, a cura del Massimario, in *Cass. pen.*, supplemento al volume LVI – giugno 2016, 278 e ss.

[41] Sul punto, nella decisione, si legge: «In realtà, alla luce del dettato normativo sopra richiamato, nella giurisprudenza di questa Corte di legittimità, anche a Sezioni Unite, si rinvengono elementi per poter affermare che il *discrimen* perché ci sia stato o meno flusso informativo e quindi debba essere applicata la disciplina delle intercettazioni e non quella del sequestro è nell'avvenuto inoltro dell'e-mail da parte del mittente».

l'introduzione di una disciplina normativa relativa all'impiego del mezzo investigativo in esame nelle investigazioni[42].

Il tema dell'uso del captatore informatico, in particolare, è stato già affrontato nel corso dei lavori parlamentari per la conversione del decreto legge 18 febbraio 2015, n. 7, "*Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale*", convertito con modificazioni dalla legge 17 aprile 2015, n. 43. In quell'occasione è stata proposta una norma con la quale si voleva modificare l'art. 266-*bis* cod. proc. pen., inserendo nella disposizione le parole *"anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico"*[43].

Secondo questa proposta di legge, dunque, il programma informatico inoculato "da remoto" in un dispositivo bersaglio costituisce uno strumento per realizzare «l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi».

Successivamente, è stato proposto un emendamento che mirava a circoscrivere l'area operativa del nuovo strumento alle indagini per i delitti di cui agli artt. 270-*bis*, 270-*ter*, 270-*quater* e 270-*quinquies* del codice penale commessi con le finalità di terrorismo di cui all'articolo 270-*sexies* del codice penale[44].

Queste proposte non sono state approvate, sebbene l'esigenza di integrare le misure di prevenzione e contrasto delle attività terroristiche, proprio con il decreto legge citato abbia portato all'introduzione di nuovi mezzi di ricerca della prova[45].

In data 2 dicembre 2015, è stata depositata alla Camera dei Deputati la proposta di legge C. 3470, intitolata *"Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche"*. Nella relazione che accompagna questa nuova proposta di legge è osservato che l'innalzamento della «minaccia terroristica» costituisce «una gravissima insidia per la sicurezza interna ed internazionale, nonché un fattore di instabilità dell'intero quadro geo-politico». Per adeguare la risposta investigativa occorre consentire l'utilizzo di «nuovi programmi informatici che permettano l'accesso da remoto ai dati presenti in un sistema informatico al fine di contrastare preventivamente i reati di terrorismo commessi mediante l'uso di tecnologie informatiche o telematiche». Con la nuova legge, pertanto, si intende garantire l'adeguamento tecnologico del sistema delle intercettazioni, prevedendo che le Forze di polizia possano utilizzare programmi informatici che consentano l'accesso ai

---

[42] Le iniziative legislative trovano il fondamento anche nei contributi dottrinali che auspicano l'intervento di una specifica normativa. Cfr., tra gli altri, MARCOLINI, *Le indagini atipiche a contenuto tecnologico nel processo penale: Una proposta*, cit.

[43] Per le critiche che sono state manifestate rispetto a questa proposta si veda, tra gli altri, SARZANA, *Dl antiterrorismo, saremo tutti spiati?*, in *www.ilfattoquotidiano.it*, 26 marzo 2015.

[44] Cfr. Proposta di modifica n. 2.206 al d.d.l. C. 2893 in riferimento all'art. 2, presentata il 26 marzo 2015 in Assemblea della Camera dall'on. Quintarelli e altri.

[45] L'art. 2 del decreto legge n. 7 del 2015, convertito con modifiche dalla legge n. 43 del 2015, in particolare, ha introdotto l'art. 234-*bis* cod. proc. pen. che consente l'acquisizione di documenti e dati informatici conservati all'estero, «anche diversi da quelli disponibili al pubblico», previo consenso, in quest'ultimo caso, del legittimo titolare. La stessa disposizione prevede il monitoraggio della rete per l'aggiornamento costante dell'elenco dei siti internet utilizzati per le attività e le condotte di cui agli artt. 270-*bis* e 270-*sexies* cod. pen.

computer da remoto, per acquisire dati presenti in un sistema informatico ritenuti utili alle indagini connesse al perseguimento di reati con finalità terroristiche. La relazione si conclude rilevando che «i tempi sembrano purtroppo maturi per compiere un ulteriore passo in avanti, prevedendo che l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrenti tra più sistemi (già prevista dall'art. 266-*bis*, comma 1, cod. proc. pen.), sia consentita anche attraverso l'impiego di strumenti o di programmi.

La proposta si compone di un solo articolo, con il quale si intende aggiungere, all'art. 266-*bis*, comma 1, cod. proc. pen., le seguenti parole: «, anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico»[46].

In data 20 aprile 2016, poi, è stata depositata alla Camera dei deputati la proposta di legge C. 3762, intitolata «Modifiche al codice di procedura penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, in materia di investigazioni e sequestri relativi a dati e comunicazioni contenuti in sistemi informatici o telematici»[47].

La relazione di accompagnamento, dopo aver definito «captatore legale» il programma informatico utilizzato nelle indagini, illustra le finalità della normativa tra cui:

- adeguare la disciplina delle intercettazioni al progresso tecnologico in tema di comunicazioni, permettendo l'apprensione delle comunicazioni che viaggiano direttamente tra i terminali di due utenti, senza attraversare una struttura centrale di commutazione[48];

- superare i problemi determinati dall'impiego di dati informatici in forma crittografata[49];

---

[46] Si segnala che sembra sussistere un certo contrasto tra il contenuto della relazione – nella quale si evoca l'attività di ricerca della prova da remoto – ed il tenore della norma di cui si chiede l'introduzione – che appare circoscritto alla disciplina di una nuova modalità di captazione dei flussi di dati tra sistemi informatici.

[47] Il primo firmatario è l'on. Quintarelli; co-firmatario l'on. Catalano.

[48] Si allude alle comunicazioni VOIP, tecnologia impiegata per esempio da *Skype*, che consente di effettuare una conversazione telefonica con una connessione internet, piuttosto che per mezzo della rete telefonica tradizionale. Le comunicazioni non passano attraverso centrali di commutazione, ma sono realizzate grazie a software, chiamati *gateways*, che instradano sulla rete pacchetti di dati contenenti le informazioni vocali codificate e compresse in forma digitale solo quando uno degli utenti collegati sta parlando. Sulle intercettazioni di queste comunicazioni informatiche, cfr. PARODI, *Voip, Skype e tecnologie d'intercettazione: quali risposte d'indagine per le nuove frontiere delle telecomunicazioni?*, in *Dir. pen. e proc*. 2008, 1309; Trogu, *Le intercettazioni di comunicazioni a mezzo Skype*, cit.

[49] Si allude a *Twitter*, *WhatsApp*, *Wechat*, *Snapchat*, *Telegram* ed a programmi similari, dapprima indicati, facilmente scaricabili dalla rete e idonei ad un uso su apparati mobili come gli *smartphone*, sia nelle piattaforme *Android* (Samsung ed altri) che *IOS* (Iphone ed Ipad).

- disciplinare le perquisizioni a distanza, cioè quelle che sono compiute per mezzo di strumenti informatici, assicurando il rispetto delle garanzie costituzionali, tra le quali è incluso anche il domicilio informatico[50];

Sul piano metodologico, le varie attività che il programma informatico consente sono distinte e ricondotte all'istituto tipico al quale sono più assimilabile. In particolare, l'art. 1 della proposta di legge prevede la possibilità di procedere, tramite captatori legali, a perquisizioni a distanza, nei soli casi in cui si procede per i reati di cui all'art. 51, comma 3-*bis*, 3-*quater* e 3 *quinquies*, cod. proc. pen., all'art. 407, comma 2, cod. proc. pen. e ai delitti di cui al capo I, titolo II, libro secondo, del codice penale (delitti dei pubblici ufficiali contro la pubblica amministrazione). Il decreto di perquisizione deve essere adottato dal Gip, il quale deve indicare, tra l'altro, le modalità che la polizia giudiziaria deve seguire per acquisire gli atti, garantendo che siano inaccessibili alle parti prima della notifica degli atti alla persona sottoposta alle indagini. Solo ove sia indispensabile per la prosecuzione delle indagini o per la cattura dei responsabili, il Gip può autorizzare il pubblico ministero a consultare i dati acquisiti. Le operazioni debbono essere compiute dalla polizia giudiziaria, che può avvalersi di esperti.

L'art. 2 disciplina il sequestro da remoto dei dati «diversi da quelli relativi al traffico telefonico o telematico», limitatamente ai reati dapprima indicati[51].

L'art. 3 modifica l'art. 266-*bis* cod. proc. pen., disciplinando l'uso dei captatori legali per compiere l'intercettazione di flussi di dati, ma anche per determinare la localizzazione geografica del dispositivo. Gli strumenti informatici, a pena di inutilizzabilità, devono possedere le caratteristiche tecniche da stabilirsi con un apposito decreto ministeriale, emanato all'esito di un procedimento al quale deve prendere parte anche l'Autorità garante per la protezione dei dati personali.

L'art. 4 prevede il carattere residuale dei nuovi mezzi investigativi, statuendo che le operazioni per mezzo del captatore informatico possano essere compiute solo quando ogni altro mezzo di ricerca della prova risulti inadeguato.

---

[50] Il "domicilio informatico", al pari del domicilio fisico, è tutelato dalla previsione della doppia riserva, di legge e di giurisdizione, ex art. 14 Cost. Tale tutela, che trova il suo fondamento in diverse disposizioni normative (Si fa riferimento, in particolare, all'art. 615-*ter* cod. pen. che, si sottolinea, è stato inserito significativamente dalla legge n. 547 del 1993 all'interno dei "delitti contro la persona", tra gli illeciti riguardanti l'inviolabilità del domicilio); nondimeno, è riconosciuta dalla stessa Corte di Cassazione (Secondo Cass., Sez. V, 8 maggio 2012 (dep. 26 ottobre 2012), n. 42021, in *Foro It.*, 2012, 12, 2, 709, *"con la previsione dell'art. 615-ter cod. pen., introdotto a seguito della L. 23 dicembre 1993, n. 547, il legislatore ha assicurato la protezione del "domicilio informatico" quale spazio ideale (ma anche fisico in cui sono contenuti i dati informatici) di pertinenza della persona, ad esso estendendo la tutela della riservatezza della sfera individuale, quale bene anche costituzionalmente protetto. Tuttavia l'art. 615 ter cod. pen. non si limita a tutelare solamente i contenuti personalissimi dei dati raccolti nei sistemi informatici protetti, ma offre una tutela più ampia che si concreta nello "jus excludendi alios", quale che sia il contenuto dei dati racchiusi in esso, purché attinente alla sfera di pensiero o all'attività, lavorativa o non, dell'utente; con la conseguenza che la tutela della legge si estende anche agli aspetti economico-patrimoniali dei dati, sia che titolare dello "jus excludendi" sia persona fisica, persona giuridica, privata o pubblica, o altro ente"*. Cfr. anche Cass., Sez. VI, 4 ottobre 1999 n. 3067 (dep. 14 dicembre 1999), in *CED Cassazione* n. 214946.

[51] L'acquisizione deve avvenire in copia, garantendone conservazione ed immodificabilità. Il giudice può disporre, con decreto motivato, il ritardo della notifica del provvedimento di sequestro.

L'art. 5 modifica l'art. 268 cod. proc. pen., stabilendo, tra l'altro, che i dati informatici acquisiti siano conservati con modalità tali da assicurare l'integrità e l'immodificabilità dei dati raccolti e la loro conformità all'originale.

L'art. 6 aggiunge il nuovo art. 89-*bis* al d. lgs. n. 271 del 1989 (norme di attuazione, di coordinamento e transitorie del codice di procedura penale), indicando i contenuti del decreto ministeriale sui captatori previsto dall'art. 3, del quale prevede l'aggiornamento ogni tre anni. Adeguandosi ad una specifica indicazione dottrinale[52], è stata prevista la necessità che il programma informatico di captazione non alteri i dati acquisiti, né le restanti funzioni del dispositivo. È previsto, inoltre, un processo di certificazione dei captatori autorizzati all'uso e presenti sul mercato attraverso sistemi di verifica che garantiscano imparzialità e segretezza e il diritto della difesa di ottenere la documentazione relative alle specifiche tecniche dei captatori. Va garantita, infine, la disinstallazione dei programmi al termine dell'uso autorizzato[53].

Da ultimo, infine, la principale delle iniziative legislative.

Si tratta del disegno di legge n. 2067, intitolato "*Modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi nonché all'ordinamento penitenziario per l'effettività rieducativa della pena*", in discussione al Senato. All'art. 35, nell'ambito della delega che si intende conferire al Governo per la modificazione della disciplina delle intercettazioni, questo disegno di legge prevede proprio la regolamentazione dell'impiego nelle indagini del captatore, rispecchiando alcune delle conclusioni cui sono pervenute le Sezioni unite, ma anche tenendo conto delle valutazioni critiche che sono state manifestate. Ad esempio, tra le prescrizioni della legge delega vi è la precisazione che l'accensione del microfono deve avvenire per mezzo di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico nel dispositivo bersaglio; la registrazione deve essere avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'art. 348, comma 4, cod. proc. pen.; il trasferimento delle registrazioni deve essere effettuato soltanto verso il *server* della Procura così da garantire originalità ed integrità delle registrazioni; l'attivazione del dispositivo deve essere sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater* cod. proc. pen.; fuori da tali casi, nei luoghi di cui all'art. 614 cod. pen., soltanto qualora ivi sia in corso l'attività criminosa. Da tale ultima indicazione deriva che s'intende consentire il ricorso a questo strumento anche fuori dai casi di reati di criminalità organizzata, seppur l'uso è circondato da ulteriori opportune cautele: il decreto autorizzativo del giudice, in particolare, deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini.

---

[52] ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, in Costabile - Attanasio (a cura di), *IISFA Memberbook 2012 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter*, Forlì 2013, 1 e ss.

[53] L'art. 7 della proposta vuole modificare l'art. 226 del d. lgs. n. 271 del 1989 (norme di attuazione, di coordinamento e transitorie del codice di procedura penale), adeguando anche la disciplina delle intercettazioni preventive al nuovo strumento di captazione informatica.

Anche in questo disegno di legge, pertanto, ritorna la centralità del provvedimento del Gip, che deve garantire il contemperamento dei diritti fondamentali confliggenti.