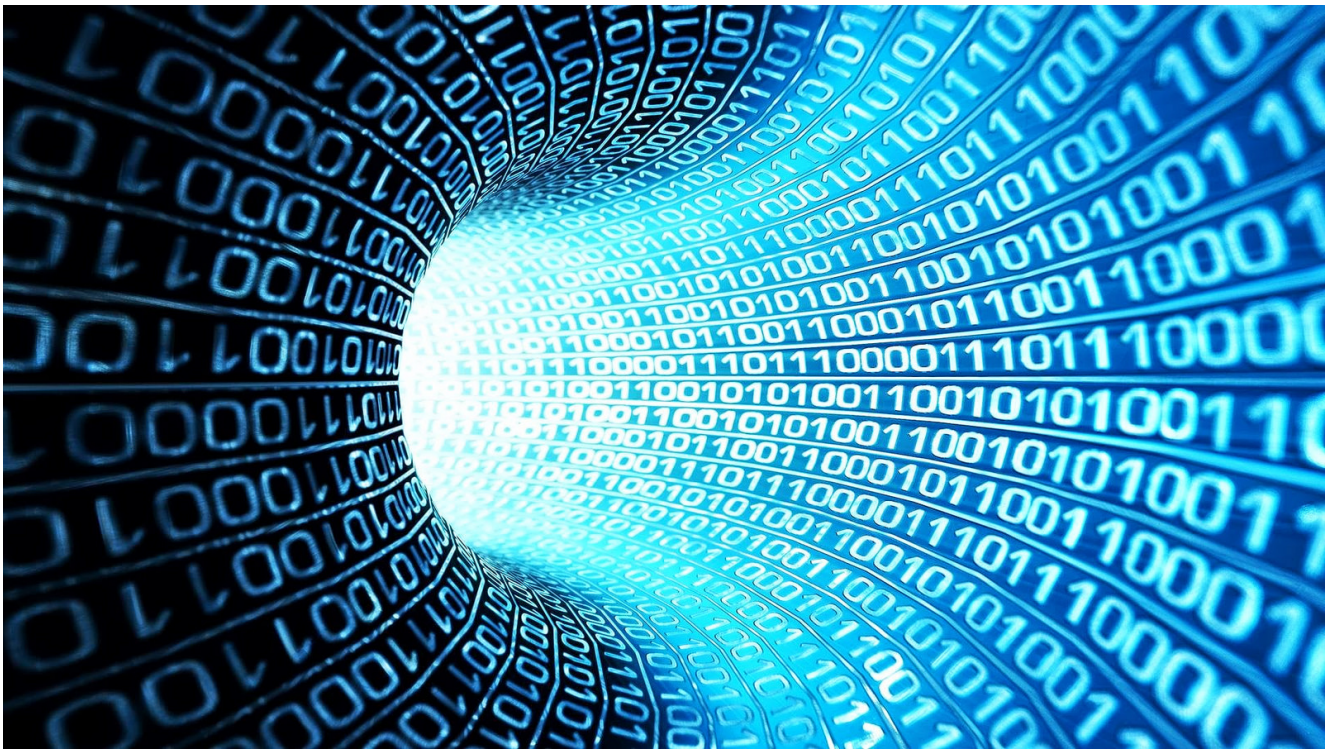
LA RIFORMA DELLE INTERCETTAZIONI: DELITTI DEI PP.UU. CONTO LA P.A E VIRUS INFORMATICO



“foto1897” di Informàtica, licenza CC BY-SA 2.0, flickr.com

Sommario: 1. Premessa. 2. La semplificazione delle condizioni di utilizzo del “paradigma intercettativo” nei più gravi reati dei pubblici ufficiali contro la pubblica amministrazione. 3. La neo introdotta disciplina legislativa del captatore informatico

1. **Premessa**

Con il d.lgs. 29 dicembre 2017, n. 216 – pubblicato in Gazzetta Ufficiale 11 gennaio 2018, n. 8 – il Governo ha dato seguito alla delega legislativa attribuitagli dall’art. 1, comma 84, l. 23 giugno 2017, n. 103.

Il *Leitmotiv* che permea la *ratio* riformatrice è posto nella

tutela della riservatezza dei soggetti solo occasionalmente coinvolti dallo strumento captativo, e come tale, almeno secondo la relazione di accomunamento del decreto, l'intera novella dovrebbe essere interpretata alla luce della predetta garanzia a tutela della *privacy*[1]. Tuttavia il «modesto ritocco»[2] apportato dal legislatore delegato, nonostante gli originali propositi, ha finito per «scontentare tutti»[3], dal momento che non ha garantito il diritto di difesa dell'imputato – e ancora prima il relativo principio di non colpevolezza – e della persona offesa dal reato.

Per rimanere ancora sul piano generale, si nota come legislatore (delegante prima e delegato poi) abbia recepito, con alcune defezioni, le linee guida dettate dal C.S.M.[4] sul tema del mezzo di ricerca della prova in oggetto, apportando tuttavia alcune novità significative che potrebbero limitare eccessivamente il diritto di difesa[5].

Soprattutto la disciplina delle intercettazioni mediante *Trojan horse* è lacunosa, essendo limitata sia dal punto di vista delle potenzialità intrusive del captatore informatico, sia da quello del dispositivo infettabile: il legislatore delegante, infatti, si è preoccupato di delegare il Governo secondo i principi dettati dalla sentenza Scurato pronunciata dalla Suprema Corte nel suo massimo consesso[6]. Una riforma, quindi, da questo punto di vista, anacronistica *ab origine*.

Il presente contributo si limiterà a trattare solo una parte della riforma recentemente intervenuta, fornendo una prima lettura della semplificazione delle condizioni di utilizzo delle intercettazioni quando si procede per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione e della neo introdotta disciplina codicistica del captatore informatico.

2. **La semplificazione delle condizioni di utilizzo del**

“paradigma intercettativo” nei più gravi reati dei pubblici ufficiali contro la pubblica amministrazione

I presupposti di applicabilità delle intercettazioni in seguito alla riforma sono rimasti sostanzialmente invariati, siccome non è stato modificato l’art. 266, comma 1, c.p.p., laddove, invece, si sono allargate le maglie per i delitti dei pubblici ufficiali contro la pubblica amministrazione[7].

Dispone infatti l’art. 6 d.lgs. 216/2017 che «nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell’art. 4 del codice di procedura penale, si applicano le disposizioni di cui all’art. 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203».[8]

Ne consegue che, «secondo il modello già sperimentato di lotta alla criminalità organizzata»[9], per tali delitti[10] il compendio accusatorio *in fieri* non dovrà basarsi su «*gravi* indizi di reato» e su di una *assoluta* indispensabilità del mezzo di ricerca della prova ai fini della *prosecuzione* delle indagini (art. 267, comma 1, c.p.p.); ma i presupposti applicativi saranno soddisfatti da un quadro indiziario sufficiente («*sufficienti* indizi»), qualora l’intercettazione è «*necessaria* ai fini dello *svolgimento* delle indagini (art. 13 d.l. 152/1991). Quindi, sufficienti e non gravi indizi di reato, necessarietà e non assoluta indispensabilità ai fini dello svolgimento (non per la prosecuzione) delle indagini.

È d’uopo notare che traspare dalla relazione di accompagnamento al decreto legislativo una disattenzione di fondo nelle intenzioni del legislatore delegato, il quale utilizza come sinonimi le differenti locuzioni di “prosecuzione” e “svolgimento”. Si legge, infatti, nella relazione citata che «si interviene, con autonoma

disposizione, per consentire alle intercettazioni, nei casi già previsti dalla legge […] sulla base dei presupposti dei sufficienti indizi di reato e della necessità per lo *svolgimento* delle indagini»[11]. Un utilizzo promiscuo di terminologia dai contorni affatto differenti, che potrebbe condurre a divergenze esegetiche sul punto in sede di prima applicazione nelle sedi giudiziarie e non solo.

Il lasso temporale di utilizzo dello strumento captativo subisce, di poi, una netta rimodulazione, laddove la legislazione speciale consente di ricorrere alle intercettazioni di comunicazioni o conversazioni telefoniche e di altre forme di telecomunicazione per un periodo iniziale di 40 giorni, con successive proroghe di 20, a fronte dei 15 giorni, con relative proroghe di 15, prescritte dal codice di rito.

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

Pare fornire una soluzione al quesito il comma 3 dell'art. 6

d.lgs. 216/2017, a mente del quale «l'intercettazione di comunicazioni tra presenti nei luoghi indicati dall'art. 614 del codice penale non può essere eseguita mediante l'inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa»[12] Ne deriva, *a contrario*, stante il tenore della norma, che qualora l'intercettazione ambientale sia disposta nel domicilio senza l'utilizzo del captatore informatico, essa sia legittima anche in assenza del *fumus perdurantis criminis****[13]***.

In definitiva, quindi, nei casi in cui si proceda per delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore nel massimo a cinque anni, potranno effettuarsi:

- intercettazioni telefoniche e ambientali – queste ultime al di fuori dai luoghi di privata dimora – qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini della prosecuzione delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20;
- intercettazioni ambientali "tradizionali" nei luoghi di privata dimora, anche in assenza di un fondato motivo per ritenere che all'interno si stia svolgendo l'attività criminosa, qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini della prosecuzione delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20;
- intercettazioni ambientali disposte con captatore informatico all'interno dei luoghi di cui all'art. 614 c.p., solamente nel caso in cui vi sia un fondato motivo di ritenere che all'interno si stia svolgendo l'attività criminosa, qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini della prosecuzione delle indagini

per un periodo iniziale di 40 giorni, prorogabile di 20.

3. **La neo introdotta disciplina legislativa del captatore informatic**

Nel paragrafo precedente si è trattato, *in limine*, del peculiare strumento intercettativo costituito dal captatore informatico[14], il cui ambito applicativo, negli ultimi anni, scevro di una disciplina legislativa di riferimento, era stato demandato alla sapiente esegesi ed evoluzione giurisprudenziale.

È bene premettere che svariate sono le funzionalità che si possono ricavare dal captatore legale[15], inoculabile all'interno di qualsiasi dispositivo *target* – portatile e fisso – dotato di una connessione *internet*, sia essa *wi-fi* sia essa *ethernet*[16]. Come brillantemente evidenziato dalla giurisprudenza[17] e dalla dottrina[18], con captatore informatico è possibile svolgere un'eterogenea congerie di attività tipiche e atipiche di indagine pesantemente intrusive delle libertà del soggetto destinatario, eziologicamente volte, come una sorta di *panopticon* benthamiano, a sorvegliare ogni atto quotidiano della vita. Infatti, con il captatore – che sfugge ad oggi ad ogni antivirus in commercio – è possibile, tra il resto: (1) attivare il microfono, intercettando le comunicazioni che avvengono tra i presenti nella portata del raggio del dispositivo *target*; (2) azionare la *webcam*, ottenendo così la possibilità realizzare *videoclip* e scattare fotografie, o solamente vedere attraverso l'occhio della telecamera; (3) captare il traffico dati, sia in arrivo sia in partenza dal dispositivo, sia esso relativo alla navigazione sia esso concernente la posta elettronica (*web mail* e *out look*); (4) prendere visione di ciò che appare sullo schermo (*screenshot*) o digitato sulla tastiera (*keylogger*); (5) perquisire l'*hard disk* ed estrarne copia.

In assenza di una disciplina specifica sul tema, le Sezioni Unite della Corte di Cassazione[19] erano giunte a sostenere, limitatamente alla potenzialità intercettativa, la legittimità di tale strumento di ricerca della prova tipico (l'intercettazione) attuato con mezzi atipici (il captatore informatico), ritenendo ammissibile finanche l'intercettazione ambientale domiciliare nel caso di procedimenti di criminalità organizzata – a cui si applica la disciplina derogatoria di cui all'art. 13 d.l. 152/1991 –, quest'ultima definita come qualsiasi reato associativo ascrivibile al protocollo di tipicità oggettiva dell'art. 416 c.p.

Il legislatore delegante, stante la delicatezza del tema in oggetto, ha tentato di farsi carico del problema, basando purtroppo il proprio orizzonte conoscitivo delle potenzialità del captatore informatico limitatamente a quanto prescritto dalla sentenza Scurato, limitando di conseguenza l'intervento riformatore esclusivamente alle funzioni di intercettazione ambientale[20]. L'art. 1, comma 84, lett. *e*, infatti, delega il Governo a «disciplinare le *intercettazioni* di comunicazioni o conversazioni *tra presenti* mediante l'immissione di captatore informatici in *dispostivi elettronici portatili*», prevedendo altresì che l'«attivazione del *microfono*» avvenga solo in seguito ad apposito comando.

La *ratio* informatrice della novella legislativa volta a tutela la riservatezza si manifesta, ancora una volta nella legge delega, con riferimento alle intercettazioni di comunicazioni o conversazioni tra presente nei luoghi di privata dimora *ex* art. 614 c.p., ammesse, in assenza del *fumus perdurantis crimis*, solamente qualora si proceda per delitti che destano particolare allarme sociale previsti dall'art. 51, commi 3 *bis* e 3 *quater*, c.p.p.

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

intercettazioni mediante inserimento di captatore informatico».

Completamente in linea con quanto previsto dalla legge delega, l'art. 4 cit. modifica l'art. 266 c.p.p. – mediante l'interpolazione del primo periodo del comma 2 e con l'introduzione *ex novo* di un comma 2 *bis* – prevedendo che la captazione di comunicazioni tra presenti possa essere posta in essere anche per mezzo del virus *Trojan horse*; tuttavia se trattasi di intercettazione ambientale domiciliare, essa è consentita solo qualora vi sia fondato motivo di ritenere che all'interno dei luoghi indicati nell'art. 614 c.p. si stia svolgendo l'attività criminosa, ovvero se si proceda per i delitti di cui all'art. 51, commi *3 bis* e 3 *quater* c.p.p.

Il legislatore, come visto, si è limitato a disciplinare l'utilizzo del captatore informatico solamente per le intercettazioni tra presenti, non intervenendo in modo alcuno sulla disciplina dell'art. 266 *bis* c.p.p., la quale consente «l'intercettazione del flusso di comunicazioni relativo a sistemi informatici[21] o telematici[22] ovvero intercorrente tra più sistemi». Può così accadere che, in virtù di alcuni programmi *trojan dual use*, si possa intercettare un flusso di comunicazioni originati da *software skype, chat, mail*, sms, mms o *VoiP*. In tali casi, secondo parte della dottrina, «l'acquisizione del dato sarebbe possibile attraverso una interazione operativa tra lo strumento di cui all'art. 266 *bis* cpp […] con quella di cui all'art. 266 co.2, primo periodo come da ultimo novellato con il decreto legislativo in commento»[23].

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

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

Vi è di più. Se il legislatore avesse disciplinato la materia come sopra auspicato, non sarebbe certamente venuto meno all'idea riformatrice di tutela della riservatezza per almeno due ordini di ragioni. In primo luogo, un'intercettazione captativa itinerante si inserisce con forza lesiva maggiore nella sfera privata del soggetto rispetto a un'intercettazione tradizionale. In secondo luogo, di poi, se vi è fondato motivo di ritenere che all'interno di un determinato luogo – anche di privata dimora – si stia svolgendo attività criminosa, l'intercettazione ambientale può in ogni caso essere disposta e il risultato a cui si perviene è il medesimo: l'acquisizione di tutto ciò che viene ascoltato all'interno del locale.

L'unica differenza è il mezzo con il quale l'intercettazione viene effettuata. In altre parole, medesimi sono i risultati, medesimo è il livello di lesione della riservatezza dei soggetti che frequentano il luogo destinatario della captazione, differente è la modalità captativa: si è in presenza di una illogicità normativa riscontrabile *ictu oculi*.

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

Inoltre, sul concetto di "dispositivo elettronico portatile" è verosimile che si aprirà un nutrito dibattito in sede giurisprudenziale e dottrinale, dal momento che vi sono alcuni dispositivi che si situano in una "zona grigia" tra la nozione di portatile e di fisso.

Il legislatore delegante ha altresì palesato la volontà di circoscrivere ulteriormente la captazione alla sola registrazione audio, desumibile dall'espresso riferimento all'«*attivazione del microfono*»[24] (art. 1, comma 84, lett. *e*, n. 1 l. 103/2017) e alla «*registrazione audio*» (art. 1, comma 84, lett. *e*, n. 2 l. 103/2017). E tale volontà traspare anche dalla relazione illustrativa al decreto legislativo[25], ma non sembra trasposta fedelmente all'interno del decreto emanato, il quale più genericamente si limita a parlare di «*intercettazioni tra presenti*» e di «*registrazioni*», utilizzando una sola volta la locuzione «*microfono*».

Quid iuris, perciò, se mediante l'utilizzo del captatore informatico inoculato in un dispositivo mobile portatile si effettuassero non solo audio registrazioni, bensì anche riprese visive? Pare essere di fronte al medesimo problema interpretativo (scaturito prima della e) definitivamente risolto dalla sentenza delle Sezioni Unite Prisco, chiamata a sciogliere la *quaestio iuris* inerente alla possibilità di

intercettare comunicazioni domiciliari *inter praesentes* con strumenti di videoripresa anziché di ripresa sonora, dal momento che le telecamere finivano e «finiscono inevitabilmente per riprendere anche comportamenti domiciliari di tipo non comunicativo, ossia per realizzare una violazione sensoriale del domicilio non regolata dalla legge»[26]. Al riguardo la Corte di Cassazione ha ritenuto legittima la pratica di effettuazione di videoriprese, precisando però che il giudice a posteriori deve vagliare se quanto ripreso rappresenti un comportamento comunicativo – in quanto tale riconducibile al paradigma intercettativo – ovvero non comunicativo, poiché in tale ultimo caso il materiale cognitivo è da ritenere inutilizzabile in giudizio.

Con la recente riforma si è di fronte al medesimo problema, con l'unica differenza che risiede nella protasi del paradigma ipotetico: se è possibile ricorrere all'intercettazione con captatore informatico effettuando audio registrazioni, allora è possibile utilizzare il medesimo strumento finanche per le riprese visive di comportamenti comunicativi? Secondo condivisibile opinione dottrinale, è d'uopo effettuare un rimando alla disciplina generale sul tema «e, nello specifico, ai principi enucleati da Cass., SS.UU., sentenza n. 26795/2006 che ha ribadito il divieto delle riprese visive di comportamenti non comunicativi avvenuti in ambito disciplinare»[27].

Al fine di garantire l'affidabilità dei dati captati e registrati, dal momento che ai sensi del novellato comma 3 *bis* dell'art. 368 c.p.p.[28] per l'avvio e la cessazione delle registrazioni l'ufficiale di PG può servirsi di persona idonee ai sensi dell'art. 348, comma 4, c.p.p., il Governo ha stabilito che la trasmissione dei dati e delle registrazioni deve essere effettuata esclusivamente verso gli impianti della Procura della Repubblica e con «controlli costanti di integrità» (art. 89, comma 2 *ter*, disp. att. c.p.p.), precisando altresì che qualora non sia possibile garantire la

catena cronologica, è necessario indicare nel verbale di cui all'art. 268 c.p. le ragioni tecniche impeditive (art. 89, comma 2 *quater*, disp. att. c.p.p.).

Per rimanere sul versante "tecnico" della materia, è necessario che il captatore informatico risponda ai requisiti tecnici richiesti e stabiliti con decreto del Ministro della Giustizia (art. 89, comma 2 *bis*, disp. att. c.p.p.) e che sia immediatamente disattivato e reso inutilizzabile al termine delle indagini (art. 89, comma 2 *quinquies*, disp. att. c.p.p.).

Quanto al regime di utilizzabilità dei dati e delle registrazioni raccolti con l'utilizzo del virus *trojan*, oltre ai casi già precedentemente inscritti nell'art. 271 c.p.p., il legislatore delegato ha introdotto un nuovo comma 1 *bis* all'articolo citato, il quale prevede due differenti e nuove cause di inutilizzabilità. Non sono utilizzabili: 1) i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico, quali, per esempio, le prove tecniche precedenti all'effettivo inizio delle operazioni; e 2) i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo[29].

Vi è, inoltre, un'ulteriore causa di inutilizzabilità dei dati raccolti in procedimenti (*rectius*: per la prova di reati) diversi da quello per cui si procede, imposta dall'art. 1, comma 84, lett. *e*, n. 7 l. 103/2017 secondo cui «i risultati intercettativi così ottenuti poss[o]no essere utilizzati ai fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e poss[o]no essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti di cui all'articolo 380 del codice di procedura penale». Il legislatore delegato, tuttavia, forse per uniformarsi al disposto dell'art. 270, comma 1, c.p.p. ha tradotto il predetto criterio direttivo formulando il nuovo comma 1 *bis* sulla falsa riga di quanto già previsto dal comma 1. Stabilisce, infatti, l'art. 270, comma 1 *bis*, c.p.p. che «i

risultati delle intercettazioni tra presenti con captatore informatico su dispositivo elettronico portatile non possono essere utilizzati per la prova di reati diversi da quelli per i quali è stato emesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza»[30].

L'unica differenza semantica tra i due commi risiede nelle locuzioni «in procedimenti diversi» e «per la prova di reati diversi». Per condivisibile opinione dottrinale, tale differenza semantica «lascia intendere un ambito di utilizzabilità minore per le intercettazioni tra presenti mediante captatore informatico»[31], dal momento che la Corte di Cassazione, nel suo massimo consesso, ha stabilito che è necessario fare riferimento a una nozione sostanziale di procedimento diverso, e tale diversità va collegata all'inesistenza di un nesso di connessione ai sensi dell'art. 12 c.p.p.[32]. E una simile interpretazione non può che uscire rafforzata dall'autonoma introduzione del comma 1 *bis* dell'art. 270 c.p.p.: diversamente opinando, infatti, il comma 1 *bis de quo* risulterebbe essere tautologico e una mera superfetazione normativa se raffrontato al comma che precede[33], privando così di autonomo significato precettivo la disposizione.

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

costituzionalmente orientata della disciplina codicistica come novellata dal d.lgs. 216/2017.

Quanto alla procedura autorizzativa dell'intercettazione captativa itinerante, si segnala un nuovo onere motivazionale – quantunque non stringente – in capo al giudice (sempre su richiesta del PM), il quale deve indicare nel decreto motivato di autorizzazione «le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini». Ben più arduo, al contrario, sarà per il GIP indicare nel decreto stesso, qualora non si proceda per i più gravi delitti associativi di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., «i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono».

Nei casi di urgenza, di poi, limitatamente ai delitti di cui all'art. 51, commi 3 *bis* e 3 *quater* c.p.p., il pubblico ministero potrà procedere autonomamente, senza attendere la previa autorizzazione del giudice e sempre che sia impossibile attendere il provvedimento dello stesso, ma con l'onere di richiederne la convalida. Anche in questo caso vi è una discrasia tra i principi direttivi del delegante e quanto effettivamente trasposto in legge dal delegato[34], dal momento che l'art. 270, comma 2 *bis*, c.p.p. impone al PM di indicare «le ragioni di urgenza» che rendono impossibile attendere l'autorizzazione del giudice; al contrario, la legge delega poneva in capo al pubblico ministero un doppio onere motivazionale ben più stringente, consistente nell'indicazione: 1) delle «specifiche situazioni di fatto che rendono impossibile la richiesta al giudice» e 2) delle «ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini». Infine, il pubblico ministero dovrà richiedere la convalida al GIP con le modalità e gli effetti di cui all'art. 270, comma 2, c.p.p., ossia dovrà trasmettere immediatamente a quest'ultimo – e comunque non oltre 24 ore – il decreto con il quale ha disposto le intercettazioni itineranti. Il giudice è

tenuto a decidere entro 48 ore dalla ricezione dalla comunicazione[35].

Pare ancora opportuno sottolineare che per i delitti di cui all'art. 51, commi 3 *bis* e 3 *quater*, c.p.p., in quanto reati associativi, si applica la disciplina derogatoria di cui all'art. 13 d.l. 152/1991, e perciò qualora sussistano sufficienti indizi di reato e il particolare strumento di ricerca della prova sia necessario ai fini della prosecuzione delle indagini per un periodo iniziale di 40 giorni, prorogabile di 20. Inoltre, la predetta disciplina si applica, solo parzialmente, come visto, anche ai più gravi reati dei pubblici ufficiali contro la pubblica amministrazione, a condizione che nei luoghi di privata dimora vi sia fondato motivo di ritenere che si stia svolgendo l'attività criminosa. In altre parole, riprendendo uno schema elaborato dalla dottrina[36], i presupposti per l'autorizzazione all'intercettazione mediante captatore informatico possono essere compendiati nei seguenti termini:

- per i delitti indicati nell'art. 266 c.p.p., ad eccezione di quelli di cui all'art. 51, commi 3*bis* e 3 *quater*, c.p.p.:
  - gravi indizi di reato;
  - assoluta indispensabilità del mezzo di ricerca della prova ai fini della prosecuzione delle indagini;
  - possibilità di utilizzare il paradigma intercettativo nei luoghi di privata dimora solo in presenza di un fondato motivo di ritener che si stia svolgendo l'attività criminosa;
  - durata di 15 giorni, con possibilità di proroghe di 15 giorni;
- per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione:
  - sufficienti indizi di reato;
  - necessarietà ai fini dello svolgimento delle

indagini;
    - possibilità di utilizzare il paradigma intercettativo nei luoghi di privata dimora solo in presenza di un fondato motivo di ritener che si stia svolgendo l'attività criminosa;
    - durata di 40 giorni, con possibilità di proroghe di 20 giorni;
- per i delitti associativi previsti dall'art. 51, commi 3 *bis* e 3 *quater*p.p.:
    - sufficienti indizi di reato;
    - necessarietà ai fini dello svolgimento delle indagini;
    - possibilità di utilizzare il paradigma intercettativo anche nei luoghi di privata dimora;
    - durata di 40 giorni, con possibilità di proroghe di 20 giorni.

Bibliografia:

- Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, pp. 483-510;
- D.M., *D. lgs. – Disposizioni in materia di intercettazione di conversazioni o comunicazioni, in attuazione dell'art. 1, legge 23 giugno 2017, n. 103 – Relazione*, in *www.giurisprudenzapenale.it*;
- Conti, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *www.penalecontemporaneo.it*;
- S.M., *Ricognizione di buone prassi in materia di intercettazioni di conversazioni*, in *www.csm.it*;
- Filippi, *Pubblicata in gazzetta la riforma delle intercettazioni*, in *www.pluris-cedam.utetgiuridica.it*, 12/01/2018;
- Granozio, *Riforma Orlando: delega su intercettazioni*, in *www.parolaalladifesa.it*;

- Paoletti, *riforma procedimento penale: la delega in materia di intercettazioni*, in *www.diritto.it*
- Prete, *Linee guida sulla nuova disciplina in tema di intercettazioni*, in *www.penalecontemporaneo.it*;
- Spangher, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *www.giurisprudenzapenale.it*, 08/01/2018;
- Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni: qualche rilievo critico*, in *www.pluris-cedam.utetgiuridica.it*, 05/01/2018.

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

[2] L. Filippi, *Pubblicata in gazzetta la riforma delle intercettazioni*, in *www.pluris-cedam.utetgiuridica.it*, 12/01/2018, p. 7.

[3] L. Filippi, *Pubblicata in gazzetta*, op. cit., p. 1.

[4] C.S.M., *Ricognizione di buone prassi in materia di intercettazioni di conversazioni*, in *www.csm.it*. Il C.S.M., nel testo citato, ha compendiato in un unico programma le diverse linee guida dettate dalle singole Procure della Repubblica, in modo tale da uniformare (sebbene in modo non vincolante, ma sicuramente autorevole) sul territorio

nazionale le prassi in tema di intercettazioni.

[5] È il caso della previsione in virtù della quale, ove le intercettazioni risultino irrilevanti o inutilizzabili, bisogna indicare solamente data, ora e dispositivo dal quale è stata ricavata.

[6] Cass., Sez. Un., 1 luglio 2016, n. 26889, Scurato, in *www.cortedicassazione.it*.

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

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

[9] C.D.M., *D. lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 11. Dettando una simile disposizione, il legislatore pare essersi preso carico dell'annoso problema del malcostume permeato all'interno della Pubblica Amministrazione

[10] Senza pretesa di esaustività si segnalano gli artt. 314, 317, 318, 319,319 *ter*, 319 *quater*, 322 commi 2 e 4, 322 *bis*, 325, 331, comma 2, c.p.

[11] C.D.M., *D. lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 11

[12] Una simile previsione è dettata al chiaro scopo di uniformare la disciplina *de qua* con quella generale in tema di intercettazioni di comunicazioni e conversazioni tra presenti con lo strumento del captatore informatico. Il legislatore, infatti, con l'intervento riformatore ha previsto che, stante l'elevata intrusività nella sfera personale del soggetto coinvolto, l'intercettazione con virus *Trojan horse* sia espletabile all'interno del domicilio solo nel caso in cui si proceda per i più gravi delitti di criminalità organizzata, di stampo mafioso, eversiva o terroristica ai sensi dell'art, 51, commi 3 *bis* e 3 *quater*, c.p.p., riducendo così l'ambito applicativo originalmente tracciato con la sentenza Scurato delle Sezioni Unite.

[13] A simile soluzione conduce anche la relazione di accompagnamento al decreto legislativo, la quale prevede che l'equiparazione con la disciplina *ex* art. 13 d.l. 152/1991 «a fronte della gravità del fenomeno criminale è realizzata anche attraverso la previsione espressa secondo cui, quando si tratta di intercettazione di comunicazioni tra presenti, nei luoghi indicati dall'art. 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» (C.D.M., *D. lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 11).

[14] Il captatore informatico è stato definito dalla dottrina come un *malware* «occultamente installato dall'inquirente su un apparecchio elettronico dotato di connessione internet attiva […], il quale consente in ogni momento all'attaccante […] di captare tutto il traffico dati (sia in entrata sia in uscita), di attivare da remoto il microfono e la telecamera registrando le attività, di perquisire gli *hard disk* e di fare copia integrale del loro contenuto, di intercettare tutto quanto digitato sulla tastiera, di fotografare le immagini e i

documenti visualizzati» (L. Annunziata, Trojan *di Stato: l'intervento delle Sezioni Unite non risolve le problematiche applicative connesse alla natura del captatore informatico*, in *Parola alla difesa*, 2016, I, p. 189).

[15] Denominato anche virus informatico, virus *trojan*, *trojan horse*, agente intrusore, *remote control system* (RCS), virus di stato

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

[17] Cass., Sez. Un., 01 luglio 2016, n. 26889, Scurato, in *www.pluris-cedam.utetgiuridica.it*.

[18] F. Caprioli, *Il "captatore informatico" come strumento di ricerca della prova in Italia*, in *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, p. 483-510.

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

criminalità organizzata, anche terroristica», secondo la precisione dell'art. 13 d.l. 13 maggio 1991, n. 152

[20] Di tale "lacuna" nella delega è ben conscio il Governo: «come si ricava dal chiaro tenore della delega e dai sopramenzionati criteri per la sua attuazione, il delegante ha inteso regolamentare uno solo degli usi del captatore informatico, quale modalità specifica di esecuzione delle intercettazioni tra presenti, ed ha ad oggetto esclusivamente dispositivi mobili portatili» (C.D.M., *D. lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 9).

[21] I sistemi informatici sono formati da elaboratori e computer connessi tra loro fisicamente da *hardware* (quasi sempre cavi) per poter scambiare dati e informazioni: è il caso dei cc.dd. *local area networks* (LAN).

[22] Trattasi di sistemi formati da reti di elaboratori non collegati in modo permanente tra loro da cavi e collegamenti fisici, ma che per comunicare tra loro utilizzano sistemi dematerializzati, quali le linee telefoniche, televisive e satellitari.

[23] F. Prete, *Linee guida sulla nuova disciplina in tema di intercettazioni*, in *www.penalecontemporaneo.it*, p. 21.

[24] Come correttamente osservato in dottrina, «la necessità di sganciare la procedura di installazione del captatore dall'effettiva ed autonoma attivazione del microfono dell'apparecchio di destinazione può soltanto dedursi implicitamente dal riferimento contenuto nel nuovo art. 267, co. 1 c.p.p.» (L. Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni: qualche rilievo critico*, in *www.pluris-cedam.utetgiuridica.it*, 05/01/2018, p. 5).

[25] «Si tratta dunque di un complesso di operazioni (alcune delle quali già praticate ove consentite dalla legislazione vigente) che la tecnologia consente di effettuare, ma che il delegante non ha inteso regolare, limitando l'ambito

dell'intervento normativo alla disciplina degli aspetti attinenti all'intercettazione audio, eseguita mediante inoculazione di dispositivo portatile (smartphone, tablet ecc.) e non anche dispositivi fissi» (C.D.M., *D. lgs. – Disposizioni in materia di intercettazione*, op. cit., p. 9).

[26] F. Caprioli, *Il "captatore informatico"*, op. cit., p. 500.

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

[28] Comma modificato in linea con quanto previsto dalla legge delega all'art. 1, comma 84, lett. *e*, n. 4.

[29] «Sul piano operativo questo comporta che il pm dovrà raccomandare alla p.g. di monitorare con appositi strumenti (g.p.s. sul telefono) gli spostamenti delle persone intercettate per poi attivare o disattivare la microspia allorquando questi abbiano fatto ingresso nei luoghi di privata dimora nei quali l'intercettazione non sia consentita» (F. Prete, *Linee guida sulla nuova disciplina in tema di intercettazioni*, op. cit., p. 25).

[30] Attenta dottrina ha osservato che la legge delega imponeva l'utilizzabilità delle risultanze intercettative per i reati di cui all'art. 380 c.p.p., mentre il decreto legislativo, uniformandosi all'art. 270, comma 1, c.p.p., ha tradotto il predetto riferimento con «arresto obbligatorio in flagranza» (L. Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni*, op. cit., p. 5). E in effetti vi sono disposizioni speciali che estendono l'area operativa della precautela a fattispecie non prese in considerazione dagli artt. 380, tra le quali si annovera, *ex multis*, l'art. 13, comma 13 *ter*, d. lgs. 25.7.1998, n. 286, ai sensi del quale è obbligatorio l'arresto (anche fuori dei casi di flagranza) dell'autore dei reati di reingresso abusivo nel territorio dello Stato.

[31] F. Prete, *Linee guida sulla nuova disciplina in tema di intercettazioni*, op. cit., p. 26. Dello stesso avviso anche L. Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni*, op. cit., p. 6.

[32] Cass., Sez. Un., 26 giugno 2014, n. 32697, in *www.pluris-cedam.utetgiuridica.it*; più recentemente Cass., Sez. III, 21 gennaio 2016, n. 2608, in *www.pluris-cedam.utetgiuridica.it*

[33] L'art. 270 comma 1 c.p.p., infatti, trattando del *genus* (intercettazioni) che ricomprende anche la *species* (intercettazione mediante l'utilizzo di captatore informatico).

[34] Così L. Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni*, op. cit., p. 6.

[35] Secondo parte della dottrina, «un ulteriore profilo di contrasto è ravvisabile nella tempistica della procedura di convalida, dal momento che il rinvio operato dall'art. 267, co. 2-*bis* c.p.p. alla disciplina contenuta nel comma precedente dilata di ventiquattro ore l'itinerario delineato dalla norma delegante, la quale indica nelle quarantotto ore successive all'emissione del decreto dispositivo dell'intercettazione "urgente" il limite entro cui esaurire la procedura di convalida» (L. Suraci, *Lo schema di dlgs di riforma della disciplina delle intercettazioni*, op. cit., p. 6).

[36] F. Prete, *Linee guida sulla nuova disciplina in tema di intercettazioni*, op. cit., pp. 22 s.