La nuova disciplina del captatore informatico tra esigenze investigative e salvaguardia dei diritti fondamentali Dalla sentenza "Scurato" alla riforma sulle intercettazioni

The new discipline of the computer sensor between investigative needs and protection of fundamental rights From "scurato" judgment to interception reform

Luigi Palmieri
Dottore di ricerca presso Università degli Studi di Salerno
lpalmieri@unisa.it

Captatore informatico, Trojan,
Intercettazioni di comunicazioni tra presenti,
Perquisizione da remoto

Abstract

Il nuovo volto della criminalità organizzata ha posto i sistemi d'indagine tradizionali in grave difficoltà, evidenziando "l'incapacità investigativa" delle Autorità Giudiziarie di contrastare, in maniera efficace, il traffico di droga e la cessione di materiale pedopornografico attraverso il web. Solo con il ricorso alle indagini informatiche gli organi investigativi sono posti in condizione di ricercare ed assicurare il dato probatorio. Il nuovo orizzonte investigativo è rappresentato dalle intercettazioni di comunicazioni tra presenti tramite captatore informatico. Si tratta, com'è noto, di un sistema che consente da remoto la captazione di immagini e suoni tramite l'inoltro di un malware sul dispositivo bersaglio. Il Legislatore ha atteso oltre dieci anni per regolamentare l'utilizzo del nuovo strumento investigativo mediante l'introduzione del D.lgs 29 dicembre 2017, n. 216. La novella raccoglie diffusamente la "proposta" della "sentenza Scurato", e solo alcune dei tanti spunti offerti dalla dottrina negli ultimi anni. Al Giudice per le indagini preliminari è affidato il compito di "recuperare" l'effettiva funzione di controllo sul "progetto investigativo" ipotizzato dal pubblico ministero al fine di salvaguardare i valori costituzionali coinvolti dall'utilizzo del mezzo.

The new face of organised crime has got the traditional systems of investigations into troubles, highlighting investigation inability of judicial authorities to combat effectively drug trade and spread of child sexual abuse material on the internet. Only through computer investigation, investigative bodies are able to seek and ensure the probative data. The new investigation horizon is interception of communications among present (and search) through computer collector. That is a system which permits image and sound collection remotely through forwarding of a malware on a target device. The legislator has been waiting for more than ten years for regulating the use of the new investigative instrument by the introduction of the Legislative Decree December 29 th 2017 n. 216. This collects largely the proposal of "Scurato" judgment and numerous suggestions offered from the doctrine in the last years. The examining Judge is responsible to recover the real control function on the investigative project hypothesized by the prosecutor in order to safeguard the constitutional values involved in the use of the mean.

Sommario

1. Introduzione.

Il rinnovato utilizzo investigativo della tecnologia ha indotto il *Legislatore* ad intervenire per adeguare – e correttamente classificare – l'attuale disciplina processuale delle intercettazioni di conversazioni tra presenti (e della perquisizione informatica) con le nuove forme di captazione da remoto, sempre più spesso utilizzate dalle Autorità Giudiziarie e non soltanto nei procedimenti che obbediscono alle deroghe previste dal *doppio binario*.

Le organizzazioni criminali (anche transnazionali) utilizzano il *web* per "traghettare" le loro attività criminose. Solo per fare un esempio, negli ultimi anni, è balzato agli onori della cronaca giudiziaria l'utilizzo del c.d. *deep web.* Si tratta di una rete telematica sommersa impiegata dal crimine organizzato per la cessione di sostanze stupefacenti, il traffico di armi, la vendita di documenti falsi e la cessione di materiale pedopornografico. Non a caso l'immagine che descrive (e contraddistingue) il *deep web* è molto suggestiva: un *icerberg*!

Al di sotto della *rete* di comune utilizzo c'è l'orrore; una superficie sommersa ove si vende e si compra – tramite *Bit Coin* – tutto ciò che è illegale, il cui accesso è possibile, semplicemente, tramite l'utilizzo di *browser* non indicizzati che non consentono l'identificazione dell'indirizzo IP dell'utente[1]. È, pertanto, innegabile che nell'era digitale *l'intrusione informatica* costituisca l'unica modalità per le Autorità Giudiziarie di penetrare i "fortini" protetti dalle organizzazioni criminali.

In primis, intendo illustrare *il divenire*[2] del nuovo orizzonte investigativo – il c.d. *captatore informatico* – e tracciare il labile confine tra diritto alla riservatezza e le asserite esigenze di ordine pubblico; verificare, dunque, la tenuta del sistema processuale alla luce dei valori costituzionali e convenzionali coinvolti dall'utilizzo del recente mezzo di ricerca della prova.

Si tratta di un sistema basato sull'invio da remoto di un *virus* autoinstallante su qualsiasi apparecchio, *smartphone, talbet, computer, smart tv*[3]. L'inoltro del *malware* consente al captante di eseguire le seguenti funzioni:

- Captazione dei dati in partenza ed in arrivo del dispositivo;
- Acquisizione di comunicazioni e conversazioni intrattenute mediante applicazione di *instant messaging* (*whatsapp, facebook messanger, instagram* e altro)
- Attivazione del microfono;
- Attivazione della webcamera;
- Perquisizione totale o parziale dell'*hard disk*;
- Decifrazione di tutto ciò che viene digitato sul dispositivo bersaglio (c.d. funzione *keylogger*);
- Geolocalizzazione e/o pedinamento elettronico.

Un *congegno bulimico*[4] che permette di gestire, in un centro remoto di comando e controllo, la captazione – spegnendo e accedendo, all'occorrenza, *microfono* e *webcam* – e, dunque, di carpire immagini e suoni prelevandoli dal dispositivo bersaglio.

Non è tutto! Mediante l'inoltro del *virus* è consentita l'ispezione/perquisizione del dispositivo intercettato (ed eventualmente anche acquisirne i contenuti) aggirando, *in toto*, le garanzie difensive previste per le tradizionali forme di perquisizione, ispezione e sequestro.

Più che di "violazione" sarebbe più corretto parlare di "attentato" al fondamentale diritto alla riservatezza; non è un caso se la dottrina si è spinta ad affermare che ascoltare e leggere uno *smartphone* rasenta il controllo psichico[5]: "*opinioni e pensieri*" prima di *"azioni e condotte*

[1] Sul tema del *deep web*, v. L. Varriale, *La prigione dell'umanità. Dal deep web al 4.0, le nuove carceri digitali,* Bologna, 2017.
[2] In dottrina v. A. Capone, *Intercettazioni e Costituzione. Problemi vecchi e nuovi wiretapping and constitution. Old and new Issues.,* in *Cass. pen.,* 2017, 3, p. 1263.
[3] L'installazione del *malware* avviene tramite l'inoltro di un *sms*, una mail o l'aggiornamento di una applicazione sul dispositivo bersaglio.
[4] L'espressione è di L. Filippi, *L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi ma sbagliano la terapia,* in *ilpenalista.it*, 6 settembre 2016.
[5] Così P. Tonini – C. Conti, *Il diritto delle prove penali,* Milano, 2014, p. 482.

concrete"[6].

Nella incessante ricerca di un difficile bilanciamento – ove si contrappongono da un lato, un'avvertita esigenza investigativa di efficace contrasto al crimine organizzato e, dall'altro, la tutela dei valori costituzionali e convenzionali coinvolti dall'utilizzo *Trojan* – la giurisprudenza di legittimità ha impiegato quasi dieci anni per fissare un primo, fragile, punt(in)o.

2. La funzione di "controllo" del decreto autorizzativo.

La questione sottoposta al vaglio del Supremo Consesso ha avuto ad oggetto la presunta illegittimità del decreto autorizzativo del captatore informatico, in tutti i luoghi ove era collocato il dispositivo bersaglio in uso all'indagato[7].

L'eccepita inutilizzabilità del contenuto delle conversazioni captate è da attribuirsi alla mancata specifica, preventiva, individuazione dei luoghi (ivi compresi quelli di privata dimora, ai sensi dell'art. 614 c.p.) in cui è stata autorizzata la captazione tra presenti[8].

La Corte ha sostenuto che la fisiologica *natura itinerante* del captatore informatico non consentisse al Giudice per le indagini preliminari di prevedere, e predeterminare, i luoghi di privata dimora e, di conseguenza, l'impossibilità per lo stesso Giudice di motivare adeguatamente il decreto autorizzativo sul "*fondato motivo che ivi si stia svolgendo attività criminosa*" (ex art. 266 c. 2 c.p.p.).

Pertanto, la S.C. ha concluso per l'inutilizzabilità dei risultati acquisiti con il *Trojan* soltanto per i procedimenti aventi ad oggetto "*reati comuni*", limitando l'impiego del captatore informatico ai soli "*reati di criminalità organizzata*"[9], laddove il luogo dell'intercettazione è normativamente indifferente - ai sensi dell'art. 13 del D.L. 152/1991 in deroga al 266 c. 2 c.p.p. – ovvero consentito in ogni imprevedibile domicilio[10].

La sentenza *Scurato*, piuttosto che segnare il definitivo superamento dei problemi interpretativi sull'ammissibilità del *captatore informatico*, ha suscitato, in dottrina, notevoli perplessità in ordine al pericolo che l'Ufficio del p.m. potesse strumentalizzare l'iscrizione per *il delitto associativo* ai solo fini di legittimare, *ex post*, l'utilizzo del mezzo di ricerca della prova[11].

Siamo, infatti, spettatori di plurimi interventi della giurisprudenza, sempre attenta a custodire l'elemento di prova nonostante il decreto autorizzativo del G.i.p. si riveli, *ex post*, disposto in palese violazione dei limiti di ammissibilità. Com'è noto, l'orientamento prevalente ha ritenuto utilizzabili i risultati delle intercettazioni, per una originaria prospettazione accusatoria – riconducibile nell'alveo della disciplina prevista dall'art. 13 c. 1 del D.L. 13 maggio 1991 n. 152 – poi riqualificata, nel prosieguo delle indagini, a fatti non ascrivibili all'area della c.d. *criminalità organizzata* [12].

Stando all'assunto proposto dalla richiamata giurisprudenza, la doverosa verifica di legalità

[6] V. in dottrina, A. Gaito-S. Furfaro, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza,* in A.A. V.V., *I principi europei del processo penale,* a cura di A. Gaito, Roma, 2016, p. 364, il quale rileva che "*nulla sfugge al controllo, e dal telefono all'intimità quotidiana, dalla corrispondenza alla rete fino alla messaggistica di WhatsApp e Blackberry tutto è ormai tecnicamente intercettabile: parole, suoni, gesti e, conseguentemente, opinioni e pensieri prima di azioni e condotte concrete*".

[7] Cfr. in giurisprudenza, Cass., Sez. un., 28 aprile 2016, Scurato, n. 26889, in *Arch. nuova proc. pen.*, 2017, p. 76. In particolare, il richiesto controllo nomofilattico può essere così sintetizzato "*se – anche nei luoghi di privata dimora ex art. 614 c.p., pure non singolarmente individuate a 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 informativo in dispositivi elettronici portatili*".

[8] In dottrina, v. diffusamente, A. Gaito – S. Furfaro, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. pen.* 2016, II, p. 309; A. Cisterna, *Spazio ed intercettazioni, una laison tormentata. Note ipogarantistiche a margine della sentenza Scurato delle Sezioni unite,* in *Arch. pen.* 2016, II, p. 331; G. Lasagni, *L'uso dei captatori informatici (trojans) nelle intercettazioni "fra presenti",* in *Dir. pen. cont.*, 7 ottobre 2016; M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p. 149.

[9] La sentenza *Scurato* ha limitato la portata del captatore informatico ai reati di criminalità organizzata, ed in particolare ha fornito una nozione ampia di "criminalità organizzata" ovvero ha chiarito che l'utilizzo del mezzo di ricerca della prova è consentito "*…non solo ai delitti elencati nell'art. 51 c. 3 bis e 3 quater c.p.p. ma anche quelli comunque facenti capo a un'associazione per delinquere ex art. 416 bis c.p., correlata alle attività più diverse, con esclusione del mero concorso di persone*".

[10] Cfr. in dottrina, L. Giordano, *La prima applicazione dei principi della sentenza "Scurato" nella giurisprudenza di legittimità*, in *Dir. pen. cont.*, fasc. 9/2017, p. 183 ss.

[11] Così L. Giordano, *Dopo le sezioni unite sul captatore informatico: avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo*, in *Dir. pen. cont.,* fasc. 3/2017, p. 177 ss.

[12] Sul punto, v. in giurisprudenza, Cass., Sez. VI, 01 marzo 2016, n. 21740, in *C.E.D. Cass,* n. 266922 secondo cui "*La legittimità di una intercettazione deve essere verificata al momento in cui la captazione è richiesta ed autorizzata, non potendosi procedere ad una sorta di controllo diacronico della sua ritualità sulla base delle risultanze derivanti dal prosieguo della captazione e dalle altre acquisizioni*". Sul tema v. anche Cass., Sez. VI, 16 maggio 1997, n.1972, in *C.E.D. Cass,* n. 21045.

del decreto autorizzativo andrebbe effettuata, *ex ante*, al momento in cui la captazione è disposta, e non assume alcun rilievo processuale, in termini sanzionatori, l'eventualità che all'esito delle indagini l'ipotesi accusatoria, inizialmente formulata, non venga, poi, confermata dalle risultanze investigative[13].

La singolare forza intrusiva del captatore informatico ha, però, indotto la giurisprudenza – nelle prime applicazioni *post* pronuncia *Scurato* – ad esaltare la funzione di garanzia del Giudice per le indagini preliminari. Il *Trojan*, infatti, esige un controllo stringente sulla imputazione provvisoria formulata dal Pubblico ministero, ovvero un obbligo di motivazione rafforzata del decreto autorizzativo che dia conto anche della corretta qualificazione giuridica del fatto[14]. In altre parole, la legalità del procedimento pretenderebbe dal "prodotto finale" un rigoroso apprezzamento sulle condotte contestate, non certo un "illecito contenitore"[15] privo del doveroso esercizio critico sulle richieste del Pubblico ministero.

Di conseguenza, la compressione dei diritti inviolabili coinvolti dall'utilizzo del *Trojan*, imporrebbe al G.i.p. l'adozione di un "modello legale di motivazione": *un'autonoma valutazione* sulle risultanze investigative poste a base della richiesta dell'Ufficio del p.m., e che escluderebbe, *a priori*, il ricorso alla tecnica della c.d. *relatio*[16].

2.1. *Le novità contenute nel d.lgs. 29 dicembre 2017, n. 216*

Nel solco tracciato dalla richiamata giurisprudenza di legittimità, il Legislatore ha regolamento il nuovo strumento investigativo mediante l'introduzione del *d.lgs.* 29 dicembre 2017, n. 216[17] che ha raccolto diffusamente la "proposta" della sentenza *Scurato*, e solo alcune delle tante riflessioni offerte dalla dottrina.

Con la modifica dell'art. 266 c. 2 c.p.p.[18], infatti, il Legislatore ha equiparato l'*itinerante captatore informatico* alle *immobili microspie* (microfoni e telecamere), sia per quel che concerne i limiti di ammissibilità e i presupposti, e sia anche per quanto riguarda il regime sanzionatorio.

Ed invero, nonostante le Sezioni Unite avessero, come innanzi detto, escluso la possibilità di ricorrere al captatore informatico per i delitti diversi da quelli di criminalità organizzata, la novella ha esteso l'ambito di applicabilità del *Trojan* anche ai delitti comuni, nei luoghi diversi da quelli previsti dall'art. 614 c.p. Per questi ultimi opera, infatti, il limite previsto dall'art. 266 c. 2 c.p.p., che ne legittima l'installazione solo se "*vi è fondato motivo che ivi si stia svolgendo l'attività criminosa*".

Quanto a presupposti e forme del decreto che autorizza l'installazione dell'agente intrusore, il nuovo art. 267 c.p.p. obbliga il Giudice a compiere l'auspicato *sforzo motivazionale*[19], ovvero indicare le ragioni che rendano necessaria tale modalità in relazione allo svolgimento delle indagini, nonché il luogo ed il tempo ove è consentita l'attivazione del microfono. Il Giudice dovrà, pertanto, adeguatamente motivare il decreto autorizzativo in ordine alla modalità di captazione prescelta ed indicare gli "ambienti" in cui la stessa dovrà avvenire, "*secondo un verosimile progetto investigativo che implica l'individuazione anche in forma indiretta dei luoghi in cui si sposterà il dispositivo mobile controllato, e sempre che si proceda per delitti diversi da quelli di*

[13] V., in dottrina, L. Kalb, *Solo l'ascolto diretto del "captato" assicura un pieno diritto di difesa*, in *Guida dir.*, 2008, 11, 43, p. 66.
[14] Cfr. sul punto, Cass., Sez. VI, 13 giugno 2017, n. 36874, in *www.iusexplorer.it*.
[15] L'espressione è utilizzata da M. Griffo, *Una proposta costituzionalmente orientata per arginare lo strapotere del captatore. Dalla sentenza Scurato alla riforma Orlando*, in *Dir. pen. cont.*, fasc. 2/2018, p. 37.
[16] Sull'uso della motivazione *per relationem* nei decreti autorizzativi delle intercettazioni, v. Corte cost., 6 novembre 1973, n. 34, in *Giur. cost.*, 1973, p. 316, con nota di V. Grevi, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*. V. in giurisprudenza, Cass., Sez. VI, 14 novembre 2016, n. 48009, in *Dir. pen. e proc.*, 2018, 1, p. 100 con nota di A. Fiaschi, *L'uso della motivazione per relationem nei decreti autorizzativi delle intercettazioni*; Cass., Sez. Un., 17 novembre 2001, n. 45189, in *Cass. pen*. 2005, p. 343. Anche la corte europea si è pronunciata sul tema, affermando che non sussiste alcuna violazione dell'art. 8 CEDU nel caso in cui il G.I.P. abbia autorizzato l'esecuzione di intercettazione ambientali mediante un provvedimento motivato *per relationem*. V. sul punto Corte Edu, 10 aprile 2000, Panarisi c. Italia.
[17] Il captatore informatico in materia di intercettazioni è oggetto della delega contenuta all'art. 1, comma 84, L. 23 giugno 2017, n. 103. c.d. *Riforma Orlando*. Per un primo commento al citato decreto legislativo v. G. Spangher, *Critiche. Certezze. Perplessità. Osservazioni a prima lettura sul recente decreto legislativo in materia di intercettazioni*, in *Giurisprudenza penale web*, 2018, p. 1.
[18] Il nuovo testo dell'art. 266 c. 2 c.p.p. recita testualmente quanto segue "*Negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile.*".
[19] L'espressione è di D. Pretti, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont.*, fasc. 1/2018, p. 219.

cui all'art. 51 c. 3 bis e 3 quater[20]".

È stato, infatti, previsto che il captante possa, da remoto, spegnere il microfono quando l'apparecchio mobile viene condotto in un luogo diverso da quello autorizzato, con l'obbligo per il personale di polizia giudiziaria di indicare l'orario di inizio e di fine registrazione (ai sensi dell'art. 348 c. 4 c.p.p.)[21].

La riforma ha aggiunto il c. 1 *bis* all'art. 270 c.p.p. che rafforza la disciplina dell'inutilizzabilità delle intercettazioni eseguite fuori dei casi consentiti dalla legge, ed in particolare senza rispettare i limiti di tempo e di luogo indicati nel decreto autorizzativo.

È presumibile che il Legislatore abbia considerato il ricorso al captatore informatico come *extrema ratio* rispetto alle tradizionali, statiche microspie. Il parametro della "necessità" legittima l'utilizzo del mezzo soltanto in via residuale, ovvero quando le altre, e meno invasive, modalità di captazione, risultino inadeguate a soddisfare l'attività investigativa richiesta nel caso concreto.

Non è escluso che il controllo di "necessità" induca il Giudice per le indagini preliminari ad applicare il principio del *minor sacrificio* mediante un controllo stringente sulla congruità della modalità di captazione richiesta dal pubblico ministero.

In altre parole, il controllo giurisdizionale si tradurrà in una diretta ingerenza sulle indagini sino a quel momento compiute, ed una prognosi sull'utilità dello strumento investigativo richiesto dal pubblico ministero.

In questa prospettiva è indispensabile il recupero della funzione di garanzia del decreto che autorizza le intercettazioni[22]: lo scrutinio dei presupposti per attivare le 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 le richieste del pubblico ministero[23].

2.2. *Il* doppio binario *per i delitti di criminalità organizzata e il* terzo binario *per quelli contro la pubblica amministrazione.*

Così come "anticipato" dalla sentenza *Scurato*, la disciplina in deroga (prevista per i delitti di cui all'art. 51 c. 3 *bis* e 3 *quater* c.p.p.) è stata, *in toto*, estesa anche al captatore informatico[24]. Il luogo ove viene autorizzata dell'intercettazione, pertanto, risulta, per espressa previsione normativa, "indifferente" ovvero sempre consentito in ossequio alla nuova disposizione di legge (*ex artt*. 266 c. 2 *bis* c.p.p.). Il Pubblico ministero, inoltre, potrà disporre l'intercettazione tra presenti a mezzo del captatore in via d'urgenza (ai sensi dell'art. 267 c. 2 *bis* c.p.p.), ma sarà gravato di un duplice onere motivazionale: il primo (preesistente alla riforma) sul "*fondato motivo di ritenere che dal ritardo possa derivare grave pregiudizio per le indagini*", ed il secondo orientato sugli elementi che impongono l'urgenza in relazione al traguardo investigativo da raggiungere ovvero "*le ragioni di urgenza che rendono impossibile attendere il provvedimento del giudice*"[25].

Inoltre, la novella ha, in parte, equiparato la disciplina delle intercettazioni prevista per i delitti di criminalità organizzata a quelli commessi dai pubblici ufficiali contro la pubblica

[20] Cfr. pag. 10 della Relazione illustrativa al D.lgs 29 dicembre 2017, n. 216.

[21] La riforma ha introdotto il c. 1 *bis* dell'art. 270 c.p.p. che rafforza la disciplina dell'inutilizzabilità delle intercettazioni eseguite fuori dei casi consentiti dalla legge ovvero al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo. V., in dottrina, L. Filippi, *L'ispe-perqui-intercettazione "itinerante,* cit.; Id., *Sub art. 267 c.p.p.*, in *Codice di procedura penale commentato*, a cura di A. Giarda-G.Spangher, V ed., p. 2620 ss.; L. Giordano, *Le intercettazioni mediante captatore informatico*, in A.A. V.V., *La riforma delle intercettazioni*, Milano, 2018, p. 45; C. Peloso, *La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo*, in *questa Rivista*, n. 1/2017, p. 149.

[22] Secondo la Corte europea, la legge nazionale che disciplina le intercettazioni di comunicazioni e conversazioni dovrebbe prevedere i casi e i modi dell'intrusione e dovrebbe, altresì, rispondere a caratteristiche tali da poter consentire l'immediata apprensione dei limiti di legittimazione al fine di consentire il controllo. Sul punto cfr. Corte Edu, 29 marzo 2005, Matheron c. Francia; Corte Edu, 15 maggio 2000, Khan c. Regno Unito; Corte Edu, 26 marzo 1987, Leander c. Svezia; Corte Edu, 26 aprile 1979, Sunday Times c. Regno Unito. In dottrina v. diffusamente sul tema A. Gaito-S.Furfaro, *Intercettazioni: esigenze di accertamento e garanzie della riservatezza,* cit., p. 374.

[23] Cfr. Cass., Sez. VI, 20 ottobre 2009, n. 50072, in *Giur. it.*, 2010, 12, p. 2649.

[24] Per quanto concerne il *c.d.* decreto d'urgenza del pubblico ministero, l'art. 267 c. 2 *bis* c.p.p. limita tale evenienza soltanto ai procedimenti per i delitti di cui all'art. 51 c. 3 *bis* e *quater* c.p.p.

[25] Ai sensi dell'art. 267 c. 2 *bis* c.p.p., il decreto dovrà essere trasmesso al giudice nei termini e con le modalità previste dall'art. 267 c. 2 c.p.p., pena l'inutilizzabilità dei risultati acquisiti.

amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni[26].

Pertanto, anche per la suddetta categoria di reati, operano le regole previste all'art. 13 del D.L. 13 maggio 1991, n. 152, ed in particolare quelle relative al periodo di durata maggiore degli ascolti, l'eventualità di attivare l'intercettazione nei luoghi di cui all'art. 614 c.p. (anche se non vi è fondato motivo che ivi si stia svolgendo l'attività criminosa) e, da ultimo, la c.d. *disciplina d'urgenza* (ai sensi dell'art. 267 c. 2 c.p.p.).

Per quanto concerne, invece, il captatore informatico, il Legislatore ha ipotizzato una sorta di *terzo binario* che si aggiunge alla disciplina ordinaria e allo statuto previsto per i delitti di criminalità organizzata[27]. Ed invero, quando si procede per i delitti commessi dai pubblici ufficiali contro la p.a., sarà invece possibile attivarlo nei luoghi di privata dimora solo ove vi sia il pericolo che ivi si stia svolgendo l'attività criminosa.

2.3. *L'inutilizzabilità dei risultati conseguiti con il* Trojan *per la prova di un "reato diverso".*

Per neutralizzare la giurisprudenza formatasi sulla c.d. *circolazione extra procedimentale*[28], il Legislatore ha ritenuto necessario inserire il c. 1 *bis* nel corpo dell'art. 270 c.p.p. che prevede l'utilizzabilità, ai fini di prova, dei risultati conseguiti con il captatore informatico, soltanto per i reati oggetto del provvedimento autorizzativo[29].

La copiosa giurisprudenza sino ad oggi intervenuta sull'art. 270 c.p.p. ha sempre sostenuto l'utilizzabilità dei risultati delle intercettazioni – telefoniche e ambientali – disposte per un titolo di reato per il quale esse sono consentite, anche quando al fatto venga, successivamente, attribuita una diversa qualificazione giuridica[30]. Il nuovo comma segna un ingiustificato *doppio binario* in tema di utilizzabilità: la sanzione colpisce, per espressa previsione normativa, solo i risultati conseguiti con il captatore informatico e non anche quelli assunti con le diverse modalità di intercettazione.

La dottrina più autorevole ha sempre ritenuto, invece, valido il divieto di utilizzabilità in caso di modifica del titolo del reato in altro che non consente l'intercettazione; il presupposto per la captazione (telefonica e ambientale) dovrebbe non solo sussistere al momento del decreto autorizzativo, ma essere anche riconosciuta dal giudice che, poi, utilizza la prova[31].

Ad ogni modo, è intuibile che la "clausola generale di chiusura" inserita del comma 1 *bis* dell'art. 270 c.p.p. "*salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza*" ha deluso le aspettative della dottrina che attendeva dal Legislatore un segnale di discontinuità rispetto alla giurisprudenza orientata al "recupero" del materiale probatorio.

3. La perquisizione da remoto.

Il decreto legislativo non è intervenuto per disciplinare la discussa utilizzabilità dei dati acquisiti mediante perquisizione da remoto attraverso il captatore informatico. Come già detto

[26] Sul punto, v. in dottrina, C. Conti, *La riservatezza delle intercettazioni nella "delega Orlando"*, in *Dir. pen. cont.,* fasc. 3/2017, p. 79 ss.; I. Coppola, *Riforma delle intercettazioni. Le nuove disposizioni per i delitti dei pubblici ufficiali contro la P.A.*, in *ilpenalista.it,* 24 gennaio 2018; L. Filippi, *Attuazione della delega sulle intercettazioni. Un'altra occasione mancata*, in *ilpenalista.it*, 29 gennaio 2018; L. Giordano, *Il Consiglio Superiore della Magistratura sulle buone prassi in materia di intercettazioni: prime considerazioni*, in *Dir. pen. cont.*, 11 ottobre 2016.

[27] A questo proposito D. Pretti, *op. cit.*, p. 228 rileva che "*le forze eccessive cautele mostrate dal legislatore in ordine alla normazione dell'agente intrusore hanno determinato quindi l'insorgenza di una terza disciplina delle intercettazioni, a metà strada tra quella ordinaria e quella speciale per reati di criminalità organizzata e terrorismo, ai quali la limitazione appena citata non si applica*".

[28] Il termine è utilizzato da D. Pretti, *Prime riflessioni*, p. 225 per indicare la giurisprudenza secondo cui l'eventuale riqualificazione derubricativa del titolo di reato rispetto al quale è stata autorizzata non pregiudica l'utilizzabilità dei risultati delle operazioni legittimamente disposte in riferimento ad un reato per il quale le medesime erano consentite.

[29] Il nuovo 270 c. 1 *bis* c.p.p. testualmente recita "*i risultati delle intercettazioni tra presenti operate con captatore informatico su dispositivo elettronico portatile non possono essere utilizzati per la prova di reati diversi da quelli per i quali è stato ammesso il decreto di autorizzazione, salvo che risultino indispensabili per l'accertamento dei delitti per i quali è obbligatorio l'arresto in flagranza*".

[30] V. in giurisprudenza Cfr. Cass., Sez. VI, 28 febbraio 2017, n. 15573, in *www.iusexplorer.it*; Cass., Sez. VI, 1 marzo 2016, n. 21740, in *C.E.D. Cass,* n. 266922; Cass., Sez. VI, 05 aprile 2012, n. 19852, in *C.E.D. Cass*, n. 252870; Cass., Sez. I, 20 febbraio 2009, n. 19852, in *C.E.D. Cass*, n. 243780; Cass., Sez. I, 19 maggio 2000, n. 24163, in *C.E.D. Cass*, n. 247943; Cass., Sez. VI, 05 aprile 2012, n. 19852, in *C.E.D. Cass*, n. 252870.

[31] Cfr. in dottrina, L. Filippi, *L'intercettazione di comunicazione*, Milano, 1997, p. 198.

in premessa, attraverso l'utilizzo del *Trojan* è consentito al captante verificare anche il contenuto dell'*hard disk*, ed eventualmente ottenere copia totale o parziale dei file ivi contenuti[32]. L'utilizzo del captatore per perquisire l'archivio di un dispositivo informatico impone di effettuare valutazioni diverse rispetto a quelle sino ad ora esposte sulla intrusione finalizzata ad intercettare flussi di comunicazioni[33]. Quest'ultima è limitata alla captazione di informazioni avente contenuto comunicativo e non anche alla mera raccolta di dati "parcheggiati" nella memoria del sistema informatico[34].

Se tale attività fosse riconducibile alla "tradizionale" perquisizione, l'interessato avrebbe diritto alla notifica dell'avviso funzionale all'assistenza difensiva (ex art. 365 c.p.p.); l'atto c.d. *garantito*, pertanto, risulterebbe, incompatibile con l'acquisizione *occulta* dei dati contenuti sul supporto informatico[35].

La giurisprudenza ha ritenuto utilizzabili i risultati conseguiti con il captatore, qualificando l'atto investigativo al pari di un *mezzo di ricerca della prova atipico* (ai sensi dell'art. 189 c.p.p.), sottraendolo alla disciplina prescritta per la perquisizione, ed alla doppia riserva di legge e di giurisdizione prevista per l'intercettazione di comunicazioni informatiche o telematiche (ex artt. 266 *bis* c.p.p.)[36]. La sentenza, comunque, ha decretato legittimo il decreto del pubblico ministero avente ad oggetto acquisizione in copia da remoto di documentazione informatica depositata nella memoria di un personal computer[37]. La Corte non si è spinta ad affrontare il tema dei connessi limiti costituzionali della prova atipica: riserva di legge, riserva di giurisdizione e la tutela del domicilio informatico, quest'ultimo sussumibile sotto il catalogo delle libertà fondamentali di rilievo costituzionale[38].

La Corte costituzionale tedesca ha evidenziato i limiti costituzionali e convenzionali dell'attività investigativa compiuta con strumenti di sorveglianza occulta che consentono anche l'acquisizione di dati da remoto[39]. La norma censurata dalla Corte – finalizzata a rafforzare il contrasto al terrorismo internazionale ed al crimine organizzato – ha attribuito al Ministro dell'Interno tedesco il potere di effettuare l'accesso segreto a sistemi informatici con l'ausilio di programmi c.d. *backdoors.* Con la citata declaratoria di incostituzionalità, infatti, la Corte ha riconosciuto il diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici ed ha, nel contempo, evidenziato che tale, invasiva, attività investigativa necessita del controllo giurisdizionale e della preventiva individuazione di presupposti e limiti temporali.

[32] Cfr. in dottrina sul punto, R. V. O. Valli, *La perquisizione informatica e la perquisizione "da remoto"*, in *il penalista.it.*, 18 ottobre 2017.
[33] Così L. Giordano, *Dopo le sezioni unite sul captatore informatico,* cit., p. 181.
[34] Cfr. in giurisprudenza, Cass., Sez. Un., 23 febbraio 2000, n. 6, D'Amuri, in *Giur. it.*, fasc. 8-9, 2001, p. 1701.
[35] L'atto tipico differisce dalla acquisizione *da remoto* anche per le finalità a cui la stessa è diretta: la ricerca *del corpo del reato* o delle *cose pertinenti al reato*. Inoltre, le disposizioni codicistiche in materia di ispezione/perquisizione prevedono il diritto del difensore di assistere al compimento dell'atto, la notifica all'indagato dell'informazione di garanzia, il deposito del verbale in segreteria, il rilascio all'interessato della copia del decreto che dispone la perquisizione. Sulla perquisizione da remoto, v. in dottrina, M. Torre, *Il captatore informatico. Nuove tecnologie investigative e rispetto delle regole processuali*, Milano, 2017, p. 56; Id., *Sistemi informatici di controllo e riservatezza. Una proposta di regolamentazione del captatore informatico,* in *ilpenalista.it*, 24 agosto 2017.
[36] Sule novità previste dal d.lgs. 29 dicembre 2017, n. 106, v. in dottrina, P. Di Geronimo-L.Giordano-A.Nocera, *La Riforma delle intercettazioni. Commento organico al d.lgs. 29.12.2017, n. 216*, Napoli, 2018; C. Parodi – N. Quaglino, *Intercettazioni*: *tutte le novità*, in *Officina del diritto*. *Il penalista*, Milano, 2018.
[37] Sul punto, Cfr. Cass., Sez. V, 14 ottobre 2009, n. 16556, Virruso, in *C.E.D. Cass*, n. 246954 così massimata "*È 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, qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del "personal computer" o che in futuro sarebbero stati memorizzati. (Nel caso di specie, l'attività autorizzata dal P.M., consistente nel prelevare e copiare documenti memorizzati sull'"hard disk" del computer in uso all'imputato, aveva avuto ad oggetto non un "flusso di comunicazioni", richiedente un dialogo con altri soggetti, ma "una relazione operativa tra microprocessore e video del sistema elettronico", ossia "un flusso unidirezionale di dati" confinati all'interno dei circuiti del computer; la S.C. ha ritenuto corretta la qualificazione dell'attività di captazione in questione quale prova atipica, sottratta alla disciplina prescritta dagli artt. 266 ss. cod. proc. pen.)".*
[38] Nel caso sottoposto al vaglio della Suprema Corte il computer oggetto della perquisizione da remoto era collocato in luogo aperto al pubblico – in particolare un ufficio comunale – ove sia gli imputati, e gli altri impiegati, avevano accesso per svolgere le loro mansioni.
[39] Così Bundersverfassungsgericht, 27 febbraio 2008, in *Riv. trim. dir. pen. econ.*, 3, 2009, p. 679, con nota di R. Flor, *Brevi riflessioni a margine della sentenza del Bundersverfassungsgerich sulla c.d. on line durchsuchung.* La Corte tedesca, con la suddetta pronuncia, ha dichiarato l'incostituzionalità di alcune disposizioni di legge che autorizzavano la polizia federale– limitatamente al delitto di terrorismo internazionale – a ricorrere a misure di sorveglianza "occulte", tra cui la perquisizione da remoto. Sul punto v. in dottrina, v. A. Balsamo, *Intercettazioni ambientali mobili e cooperazione giudiziaria internazionale: le indicazioni desumibili dalla giurisprudenza della Corte di Strasburgo*, in *Cass. pen.*, 2016, 11, p. 4236; A.Venegoni – L. Giordano, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *Dir. pen. cont.*, 8 maggio 2016; L. Giordano, *Dopo le sezioni unite sul captatore informatico,* cit., p. 181; F. Iovene, *Le c.d. perquisizioni on line: tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *questa Rivista*, 3-4/2014; M. Torre, *Il virus di Stato nel diritto vivente tra esigenza investigative e tutela dei diritti fondamentali,* in *Dir. pen. proc.*, 2015, p. 1163; R. V. O. Valli, *La perquisizione informatica*, cit., p. 6.

L'emergenza terrorismo internazionale ha indotto, successivamente, il Legislatore tedesco ad introdurre una legge con la quale ha assegnato alla polizia federale poteri investigativi di sorveglianza occulta da remoto.

Pertanto, la Corte federale, nel dichiarare incostituzionale anche la suddetta norma, ha evidenziato il "conflitto" tra l'attività di *intelligence* da remoto e il principio di proporzionalità, alla cui stregua va compiuto il bilanciamento tra poteri pubblici e prerogative individuali[40].

Dello stesso avviso è anche la Corte europea dei diritti dell'uomo[41] che ha fornito importanti indicazioni sui requisiti *qualitativi e contenutistici*[42] che deve rivestire la normativa nazionale in materia di attività investigativa da remoto. La Corte ha sottolineato la necessità di adottare regole chiare e dettagliate sul tema: stringenti limiti di ammissibilità, durata delle misure di sorveglianza, controllo giurisdizionale e modalità di conservazione dei dati acquisiti[43].

I segnali provenienti dall'Europa dovrebbero indurre il *Legislatore* di intervenire quanto prima per fornire una corretta qualificazione giuridica della perquisizione mediante l'introduzione di uno specifico ed autonomo mezzo di ricerca della prova. La regolamentazione dovrebbe, pertanto, introdurre l'autorizzazione motivata del Giudice per le indagini preliminari, e delimitare l'utilizzo del mezzo ad una ristretta categoria di delitti.

Sarebbe auspicabile, altresì, la previsione di modalità e tecniche dirette ad assicurare la conservazione dei dati originali ed impedirne l'alterazione, al fine di garantirne l'attendibilità e consentire, *ex post*, l'esercizio del diritto di difesa sulle operazioni compiute[44]. L'assenza di contraddittorio al momento del compimento dell'atto, e il sacrificio dei diritti coinvolti dall'utilizzo dello strumento informatico, implicherebbe la presenza della giurisdizione per vigilare sul suo corretto utilizzo.

[40] Bundersverfassungsgerich, I Senato, 20 aprile 2016 – 1 BVR 966/09, 1 BVR 1140/09 con nota di A. Venegoni – L. Giordano, *op. cit.*, 8 maggio 2016.
[41] V. sul punto, Corte Edu, 4 dicembre 2015, Zakharov c. Russia.
[42] L'espressione è utilizzata da A. Balsamo, *Le intercettazioni mediante virus informatico tra processo penale italiano e Corte europea*, in *Cass. pen.*, 2016, 5, p. 2274.
[43] Così A. Balsamo, *op. cit.*, 2277.
[44] V. sul punto, A. Capone, *Intercettazioni e Costituzione.*, cit., p. 1267; M. Torre, *Il captatore informatico*, cit., p. 149.