Il "captatore informatico" come strumento di ricerca della prova in Italia

"Trojan horse" malware as a mean for obtaining evidence in Italy

O "captador informático" como instrumento de busca da prova na Itália

Francesco Caprioli
Professore Ordinario di Diritto processuale penale
Università degli Studi di Torino/Itália
francesco.caprioli@unito.it
orcid.org/0000-0003-4038-809X

Abstract: Il codice italiano di procedura penale non contiene alcuna disciplina delle indagini effettuate con l'ausilio di *malwares* del tipo "cavallo di Troia" installati in un dispositivo elettronico come uno *smartphone* o un *tablet*. Questo articolo spiega in quali casi, e a quali condizioni, atti investigativi di questo genere possono essere ugualmente considerati ammissibili secondo la legge processuale italiana, e illustra i contenuti dei principali progetti di riforma concernenti questa materia che sono attualmente in discussione nel Parlamento italiano.

Parole chiave: prova; indagini preliminari; perquisizioni *online*; sorveglianza *online*; intercettazione di conversazioni o comunicazioni.

Abstract: *The Italian code of criminal procedure doesn't regulate investigations realized with "Trojan horse" malwares located in an electronic device like a smartphone or a tablet. This study explains in which cases, and under what conditions, investigations like these can be nevertheless considered as admissible according to the Italian procedural law, and reports the contents of the main legislative proposals concerning this matter that are currently being discussed in the Italian Parliament.*

Keywords: *evidence; preliminary investigations; online searches; online surveillances; interception of conversations or communications.*

Resumo: *O Código de Processo Penal italiano não contém qualquer disciplina sobre a investigação efetuada com o auxílio de malwares de tipo "cavalo de Troia" instalados em um dispositivo eletrônico como um smartphone ou um tablet. Este artigo explica em quais casos, e sob quais condições, atos investigativos desse tipo podem ser, contudo, considerados admissíveis, segundo a lei processual italiana, e analisa o conteúdo dos principais projetos de reforma legislativa relacionados a tal matéria que estão atualmente em discussão no Parlamento italiano.*

Palavras-chave: *prova; investigação preliminar; busca e apreensão on line; vigilância on line; interceptação de conversas e comunicações.*

1. Una tecnica investigativa penale sempre più diffusa in Italia è quella che consiste nell'installare occultamente su un dispositivo elettronico (*smartphone*, *tablet*, *personal computer*) un *malicious software* in grado di svolgere attività di ricerca e sorveglianza online.

Inoculato nel dispositivo-*target* tramite accesso fisico o, più frequentemente, da remoto (ad esempio attraverso l'allegato di una email, un sms o un'applicazione di aggiornamento), il *virus* captatore permette agli inquirenti sia di acquisire dati già salvati e precostituiti nel sistema informatico (*online search*), sia di carpire il flusso informativo che intercorre tra il microprocessore del dispositivo sorvegliato e le sue periferiche (video, tastiera, microfono, *webcam*, ecc.), accedendo in tempo reale non solo a ciò che viene visualizzato sullo schermo o digitato sulla tastiera, ma anche ai suoni e alle immagini che entrano nell'orbita percettiva del microfono o della *webcam* (*online surveillance*). Queste, più nel dettaglio, le sue funzioni, così come recentemente descritte in una sentenza delle Sezioni unite della Corte di cassazione: «1) captare tutto il traffico dati in arrivo o in partenza dal dispositivo "infettato" (navi-

gazione e posta elettronica, sia *web mail*, che *out look*); 2) attivare il microfono e, dunque, apprendere per tale via i colloqui che si svolgono nello spazio che circonda il soggetto che ha la disponibilità materiale del dispositivo, ovunque egli si trovi; 3) mettere in funzione la *web camera*, permettendo di carpire le immagini; 4) perquisire l'*hard disk* e fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira; 5) decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*)»[1].

Naturalmente si tratta di funzioni che possono essere calibrate alle esigenze del caso specifico con opportuni accorgimenti tecnici (ad esempio, inibendo *a priori* taluni utilizzi del *malware*[2], oppure attivandolo da remoto solo in determinate circostanze). Ciò non toglie che si tratti di uno strumento probatorio dalle formidabili capacità di penetrazione nella sfera privata dell'individuo, che impone, come giustamente osserva la Corte di legittimità, «un delicato bilanciamento delle esigenze investigative con la garanzia dei diritti individuali, che possono subire gravi lesioni»[3].

2. Nel codice di procedura penale italiano manca una specifica regolamentazione della materia. Va tuttavia immediatamente precisato

---

1 Cass., Sez. un., 28 aprile 2016, Scurato, <www.penalecontemporaneo.it>, 4 luglio 2016, p. 8. Ultimo accesso: 8 aprile 2017. Una descrizione analoga è contenuta nella Relazione alla proposta di legge C. 4260 (primo firmatario l'on. Quintarelli) depositata alla Camera dei deputati in data 31 gennaio 2017 (*Modifiche al codice di procedura penale e altre disposizioni concernenti la disciplina dell'intercettazione di comunicazioni telematiche e dell'acquisizione di dati ad esse relativi*): «attualmente, i software disponibili consentono al loro utilizzatore il pieno controllo del dispositivo e, quindi, di fare telefonate, mandare SMS e leggerne l'archivio, accedere e inviare posta elettronica, tracciare la posizione GPS, attivare il microfono per ascoltare, attivare la telecamera per vedere e scattare foto, inserire, modificare e copiare (documenti, mail, foto, registrazioni, ecc.), nonché tracciare consultazioni web. Inoltre, attraverso i dispositivi, si potrebbe accedere anche ad archivi personali ed aziendali posti al di fuori del dispositivo (*server*, *cloud*, ecc.), ove viene archiviata – di fatto – tutta la vita di una persona».

2 Cfr. Procura Generale presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni unite del 28 aprile 2016*, <www.penalecontemporaneo.it>, 4 luglio 2016, p. 5. Ultimo accesso: 2 aprile 2017.

3 Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 9.

che ciò non significa che le attività investigative di cui si discute debbano ritenersi vietate, e, come tali, insuscettibili di fornire materiali probatori utilizzabili in giudizio (art. 191 c.p.p.). Ciò per due ragioni. In primo luogo, perché alcune di tali attività, come vedremo, sono riconducibili a strumenti di ricerca della prova già disciplinati dalla legge (segnatamente, l'intercettazione di comunicazioni). In secondo luogo, e comunque, perché nel sistema processuale penale italiano non esiste un principio di tassatività della prova, essendo il giudice espressamente autorizzato ad assumere anche «prove non disciplinate dalla legge» (art. 189 c.p.p.)[4]. Al cospetto di una prova "atipica", la legge processuale vuole soltanto che siano rispettate tre condizioni: 1) deve trattarsi di una prova «idonea ad assicurare l'accertamento dei fatti»; 2) la sua assunzione non deve «pregiudica[re] la libertà morale della persona» interessata; 3) prima di procedere all'ammissione, il giudice deve «sentire le parti sulle modalità di assunzione della prova».

Nel caso dei *trojan horses*, è fuori discussione che si tratti di prove idonee ad assicurare l'accertamento dei fatti. L'utilizzo del *virus* informatico non sembra inoltre in grado di "pregiudicare la libertà morale" (*id est*, di condizionare i comportamenti) delle persone coinvolte nell'indagine. Quanto alla necessità di «sentire le parti sulle modalità di assunzione della prova», è pur vero che un interpello preventivo dell'indagato non è in questo caso ipotizzabile, trattandosi di attività investigative occulte, ma è opinione diffusa in dottrina che l'art. 189 c.p.p. possa dirsi rispettato anche se il contraddittorio sulle modalità acquisitive della prova avviene a posteriori, al momento dell'utilizzo dibattimentale dei materiali probatori ottenuti per mezzo dello strumento atipico di ricerca della prova[5]. Dunque, in linea di principio, le indagini svolte per mezzo dei captatori informatici possono ritenersi ammissibili anche se non regolate dalla legge.

---

[4] Nel senso che l'art. 189 c.p.p. andrebbe inteso «in senso ampio, come comprensivo [anche] dei mezzi di ricerca della prova e dei mezzi di indagine non previsti dalla legge», cfr., per tutte, Cass., Sez. IV, 16 marzo 2000, Viskovic, *Diritto processuale penale*, 2001, p. 89.

[5] Sul punto, per maggiori approfondimenti, cfr. CAPRIOLI, Francesco. Riprese visive nel domicilio e intercettazione "per immagini", *Giurisprudenza costituzionale*, 2003, p. 2187 s.

Esiste, tuttavia, uno specifico ambito nel quale la legge italiana non ammette prove e investigazioni "atipiche". Si tratta delle prove e delle investigazioni che incidono sui tre diritti che il titolo primo della parte prima della Costituzione italiana definisce "inviolabili": il diritto alla libertà personale (art. 13 Cost.), il diritto all'intimità domiciliare (art. 14 Cost.) e il diritto alla libertà e alla segretezza delle comunicazioni (art. 15 Cost.). Tutte le attività probatorie che comportano una violazione di questi tre fondamentali diritti dell'individuo devono essere previste tassativamente dalla legge. Gli artt. 13, 14 e 15 della Costituzione italiana stabiliscono infatti che non è consentita alcuna limitazione di tali diritti – neppure nel corso di un'indagine o di un processo penale – se non per atto motivato dell'autorità giudiziaria (*riserva di giurisdizione*) e «nei casi e modi previsti dalla legge», ovvero «con le garanzie stabilite dalla legge» (*riserva di legge*). In altre parole, occorre che sia la legge ordinaria a stabilire con precisione in quali casi, con quali modalità e con quali garanzie i diritti di cui si tratta possono essere violati (e tra le garanzie previste dalla legge deve figurare anche il provvedimento motivato dell'autorità giudiziaria). Analogamente, l'art. 8 della Convenzione Europea dei diritti dell'uomo impone che sia «prevista dalla legge» ogni intrusione dell'autorità pubblica non solo nell'intimità della corrispondenza e del domicilio, ma in genere nella "vita privata" dell'individuo[6].

---

[6] «Ogni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Non può aversi interferenza di una autorità pubblica nell'esercizio di questo diritto a meno che questa ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la sicurezza pubblica, per il benessere economico del paese, per la difesa dell'ordine e la prevenzione dei reati, per la protezione della salute o della morale o per la protezione dei diritti e delle libertà degli altri». Secondo la Corte Europea dei diritti dell'uomo, la nozione di vita privata «è ampia e non suscettibile di una definizione esaustiva», e la base legale dell'atto intrusivo può essere di qualunque tipo (dai principi generali del diritto alle circolari amministrative fino al diritto non scritto, di matrice giurisprudenziale). L'importante è che l'ingerenza sia «ragionevolmente preventivabile» dal cittadino, e che questi, di conseguenza, sia «in grado di regolare la sua condotta» in proposito. Inoltre, la qualità delle fattispecie limitative, la loro chiarezza e precisione, il livello di dettaglio possono variare in relazione al grado di intrusività della misura stessa. Sul punto IOVENE, Federica. Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale, *Rivista trimestrale Diritto penale contemporaneo*, 2014, 3-4, p. 336 s.

Secondo un'autorevole opinione dottrinale, ciò significa che l'art. 189 c.p.p. andrebbe ritenuto costituzionalmente illegittimo nella parte in cui consente l'assunzione di prove atipiche che siano lesive del diritto alla libertà personale, del diritto all'intimità del domicilio o del diritto alla libertà e segretezza delle comunicazioni. Tali prove, tuttavia, andrebbero considerate ammissibili fino a che l'art. 189 c.p.p. non verrà dichiarato parzialmente illegittimo dalla Corte costituzionale[7]. L'indirizzo prevalente in dottrina – nonché nella stessa giurisprudenza della Corte costituzionale e della Corte di cassazione – è invece di segno contrario: in assenza di una predeterminazione normativa dei "casi" e dei "modi" di aggressione ai diritti fondamentali dell'individuo, la prova non regolata dalla legge che comporti una limitazione di tali diritti sarebbe da considerare *tout court* inammissibile. Ciò in quanto – hanno ribadito le Sezioni unite della Corte di cassazione in una importante sentenza del 2006 – l'art. 189 c.p.p. «presuppone logicamente la formazione lecita della prova, e soltanto in questo caso la rende ammissibile»[8].

Accolta questa premessa, occorre dunque chiedersi se le investigazioni penali effettuate con l'ausilio dei *virus trojan* siano o meno lesive dei diritti individuali protetti dagli artt. 13-15 Cost. (segnatamente, dell'intimità domiciliare e della segretezza delle comunicazioni, poiché non sembra potersi ipotizzare una violazione della libertà personale) e dall'art. 8 della Convenzione europea dei diritti dell'uomo. Se la risposta è negativa, nulla vieta, in linea di principio, di ritenere ammissibili le investigazioni di cui si tratta, anche in difetto di una specifica base legale. Se la risposta è positiva, invece, delle due l'una: o si ritiene che siano attività di indagine inquadrabili in fattispecie investigative e probatorie già positivamente regolate dalla legge processuale, e in questo caso la loro ammissibilità dipenderà dal rispetto delle condizioni dettate per l'attività tipica; o si ritiene che manchi una regolamentazione normativa, e allora, in accordo con le premesse accolte dalla Corte costituzionale e dalla Corte di cassazione, la diagnosi di ammissibilità non potrà che essere sfavorevole.

---

[7] CORDERO, Franco. *Procedura penale*, Milano: Giuffrè, 2003, p. 848.

[8] Cass., Sez. un., 28 marzo 2006, Prisco, *Cassazione penale*, 2006, p. 3943.

3. All'interno di queste coordinate concettuali si inscrive un prima problema che deve essere affrontato, concernente l'ammissibilità degli atti di *online search* compiuti con l'ausilio dell'agente intrusore informatico. Il riferimento è alle attività, già menzionate in precedenza, che consistono nel «perquisire l'*hard disk* e fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira»[9].

Simili attività non sono inquadrabili nello schema tipico della perquisizione: né in quello della perquisizione "ordinaria" regolata dagli artt. 247-252 c.p.p., né in quello della c.d. perquisizione "informatica" di cui all'art. 247 comma 1-*bis* c.p.p. Ciò per molteplici ragioni, puntualmente individuate dalla dottrina e dalla giurisprudenza. In primo luogo, perché, a differenza delle perquisizioni regolate dalla legge, sono attività investigative occulte, svolte all'insaputa della persona che ha la disponibilità dell'oggetto da perquisire. In secondo luogo, perché sono attività investigative permanenti, destinate a protrarsi nel tempo. In terzo luogo, perché sono attività investigative funzionali all'acquisizione indiscriminata di dati (notizie di reato comprese) anziché alla ricerca selettiva di prove in ordine a un addebito preesistente[10]. Si tratta dunque di investigazioni atipiche: ammissibili, come detto, se non si ritengono coinvolti diritti fondamentali dell'individuo; inammissibili nel caso contrario, almeno secondo la prevalente opinione dottrinale e giurisprudenziale.

La giurisprudenza italiana si è finora espressa nel senso dell'ammissibilità, ritenendo che l'acquisizione di dati a carattere non comunicativo per mezzo del captatore informatico non incida su alcun diritto costituzionale coperto dalla doppia riserva di legge e di giurisdizione[11]. Non tutti, però, condividono questa premessa: secondo una diffusa opi-

---

9 Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 8.

10 Cfr. TESTAGUZZA, Alessandra. I sistemi di controllo remoto: fra normativa e prassi, *Diritto penale e processo*, 2014, p. 759; TROGU, Mauro. Sorveglianza e "perquisizioni" online su materiale informatico, *In*: SCALFATI, Adolfo (a cura di). *Le indagini atipiche*. Torino: Giappichelli, 2014, p. 444. In giurisprudenza, Cass., Sez. IV, 17 aprile 2012, Ryanair, *Cassazione penale*, 2013, p. 1523 s.

11 La perquisizione *online* potrebbe dunque essere disposta con provvedimento motivato del pubblico ministero, senza coinvolgimento del giudice per le indagini preliminari: Cass., Sez. V, 14 ottobre 2009, Virruso, <www.italgiure.giustizia.it>, Massime penali Corte Cassazione, n. 246954. Ultimo accesso: 8 aprile 2017.

nione, atti intrusivi come quelli di cui si discute rappresenterebbero una nuova e peculiare forma di violazione del domicilio, riconducibile a pieno titolo nell'orbita precettiva dell'art. 14 Cost.

Che la tutela costituzionale del domicilio possa estendersi anche al c.d. "domicilio informatico" – ossia allo spazio virtuale che ciascun individuo occupa nell'universo digitale – non è, in verità, un'idea nuova: quando il legislatore italiano, molti anni fa, ha introdotto nel codice penale il reato di accesso abusivo a un sistema informatico o telematico[12], non ha esitato a inserire questa e altre analoghe fattispecie di reato nella sezione quarta del libro secondo del codice, dedicata proprio ai delitti contro l'inviolabilità del domicilio[13]. La stessa logica ispira una recente proposta di legge in materia di captatori informatici[14], nella cui relazione si trova scritto a chiare lettere che «le captazioni da remoto incidono sull'inviolabilità del domicilio», con la precisazione che «non si tratta, ovviamente, del domicilio fisico, ma del domicilio informatico, ossia quello spazio immateriale, delimitato da informazioni, nel quale una persona esplica attività legate alla vita privata o di relazione, e dall'accesso al quale il titolare ha diritto di escludere terzi».

Questo modo di ragionare corrisponde a un'esigenza di tutela dei diritti individuali di *privacy* della quale l'ordinamento deve sicuramente farsi carico. Secondo due celebri definizioni dottrinali, gli artt. 14 e 15 della Costituzione italiana offrirebbero protezione al domicilio fisico e alle comunicazioni riservate in quanto, rispettivamente, «proiezione spaziale»[15] e «proiezione spirituale»[16] della persona. Se questo è vero, si può

---

[12] Art. 615-*ter* c.p., introdotto dall'art. 4 della legge 23 dicembre 1993, n. 547.

[13] Nel senso che i sistemi informatici rappresentano «un'espansione ideale dell'area di rispetto pertinente al soggetto interessato, garantita dall'art. 14 Cost. e penalmente tutelata nei suoi aspetti più essenziali e tradizionali dagli artt. 614 e 615», cfr. Cass., Sez. V, 28 ottobre 2015, Bastoni, <www.italgiure.giustizia.it>, Massime penali Corte Cassazione, n. 266182. Ultimo accesso: 8 aprile 2017 (riferita a un'ipotesi di accesso abusivo a una casella di posta elettronica privata), che cita, al riguardo, la Relazione al disegno di legge n. 2773, sfociato nella legge n. 547 del 1993.

[14] Il riferimento è alla proposta di legge C. 4260 (primo firmatario l'on. Quintarelli) depositata alla Camera dei deputati in data 31 gennaio 2017 (v. *supra*, nota 1).

[15] AMORTH, Antonio. *La costituzione italiana*, Milano: Giuffré, 1948, p. 62.

[16] BRICOLA, Franco. Prospettive e limiti della tutela penale della riservatezza, *Rivista italiana diritto e procedura penale*, 1967, p. 1120.

ben dire che esista ormai anche una proiezione *informatica* dell'individuo, destinata ad allargare i confini del diritto all'intimità della vita privata e al rispetto della dignità personale: un nuovo ed ulteriore spazio virtuale al cui interno – esattamente come nel domicilio e nei circuiti comunicativi riservati – ciascuno deve essere in grado di manifestare e sviluppare liberamente la propria personalità, al riparo da occhi e orecchi indiscreti.

Che una simile esigenza di tutela possa essere soddisfatta facendo leva sulle norme sovraordinarie dettate a salvaguardia dell'intimità domiciliare, non è, tuttavia, altrettanto pacifico nella dottrina italiana ed europea. In una nota decisione del 2008, la Corte costituzionale tedesca ha negato che l'art. 13 della Legge fondamentale (*Inviolabilità del domicilio*) possa venire invocato per difendere i cittadini anche dalle perquisizioni *online*. Secondo i giudici tedeschi, esisterebbe, piuttosto, un autonomo diritto dell'individuo «*all'uso riservato e confidenziale delle tecnologie informatiche*», implicito nella tutela che l'art. 1 della *Grundgesetz* assicura alla dignità dell'uomo[17]. Una parte della dottrina italiana ritiene che sia questa la strada da seguire anche nell'ordinamento nazionale: la Corte costituzionale dovrebbe estrapolare dall'art. 2 della Costituzione – inteso come catalogo "aperto" di diritti inviolabili dell'individuo[18] – un nuovo diritto fondamentale alla "riservatezza informatica"[19]. L'obiezione è che in questo modo rimarrebbero interamente da definire i contorni della tutela sovraordinaria: in particolare, non si tratterebbe di un diritto esplicitamente presidiato dalla doppia riserva di legge e giurisdizione[20]. Tra gli studiosi che propendono per

---

[17] Cfr. Bundesverfassungsgericht, 27 febbraio 2008, *Rivista trimestrale diritto penale economia*, 2009, p. 679. V. anche, più di recente, Bundesverfassungsgericht, 20 aprile 2016, <www.penalecontemporaneo.it>, 8 maggio 2016, con nota di VENEGONI, Andrea; GIORDANO, Luigi. La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici.

[18] Secondo l'art. 2 della Costituzione italiana, «la Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità».

[19] ORLANDI, Renzo. Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici, *Archivio penale* (bollettino web), 25 luglio 2016. Ultimo accesso: 5 aprile 2017.

[20] «Il richiamo al solo art. 2 Cost. mostra i suoi limiti: tale norma, infatti, contrariamente agli artt. 13, 14 e 15 Cost., non individua i presupposti di una

questa ipotesi ricostruttiva v'è dunque chi suggerisce di ricercare il fondamento del diritto alla "riservatezza informatica" non soltanto nell'art. 2 Cost., ma anche nell'art. 8 della Convenzione europea[21] – da intendere, in questo specifico ambito, in senso particolarmente rigoroso quanto a livello qualitativo della base legale[22] –, per desumerne che anche il diritto di cui trattasi potrebbe essere limitato, nel nostro ordinamento, «solo nel rispetto della riserva di legge e di giurisdizione, alla luce del principio di proporzionalità»[23].

4. Tra le molteplici attività investigative che possono essere svolte per il tramite del dispositivo elettronico infettato dal *virus trojan*, una particolare attenzione va riservata a quelle che consistono nella trasformazione del suddetto dispositivo in strumento di percezione occulta di suoni e immagini[24]: ossia nell'attivare il microfono e la *webcam*, per sentire e vedere ciò che "sente" e "vede" il dispositivo.

Quando i suoni e le immagini captate documentano comportamenti comunicativi, l'atto investigativo sembrerebbe ricadere a pieno

---

limitazione da parte della pubblica autorità dei diritti inviolabili ivi sanciti»: così IOVENE, Federica. Le c.d. perquisizioni online, cit., p. 336.

21 Nonché negli artt. 7 e 52 della Carta dei Diritti Fondamentali dell'Unione Europea (CDFUE), che dopo il Trattato di Lisbona ha efficacia giuridica vincolante per gli Stati membri dell'UE, sia pure nelle sole materie di competenza dell'Unione. Cfr. IOVENE, Federica. Le c.d. perquisizioni online, cit., p. 337.

22 V. *supra*, nota 6.

23 IOVENE, Federica. Le c.d. perquisizioni online, cit., p. 338. Su posizioni analoghe FELICIONI, Paola. L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma, *Processo penale e giustizia*, 2016, p. 125 s., e LASAGNI, Giulia. L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti", <www.penalecontemporaneo.it>, 7 ottobre 2016, p. 15 s. Ultimo accesso: 1 aprile 2017.

24 Non saranno qui analizzati gli altri possibili impieghi del captatore informatico in funzione investigativa. Per un quadro più ampio cfr. CAJANI, Francesco. Odissea del captatore informatico, *Cassazione penale*, 2016, p. 4140; FILIPPI, Leonardo. L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia, *Archivio penale*, 2016, n. 2, p. 1 s.; GIORDANO, Luigi. Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo, <www.penalecontemporaneo.it>, 20 marzo 2017, p. 9 s. Ultimo accesso:1 aprile 2017.

titolo nella fattispecie dell'intercettazione di comunicazioni (artt. 266-271 c.p.p.), ossia presentarsi come una particolare modalità di espletamento di un'attività tipica di ricerca della prova. Occorre precisare che il *virus trojan* consente di intercettare sia comunicazioni effettuate per mezzo dello stesso dispositivo sorvegliato (ivi comprese le comunicazioni vocali VOIP, destinate a transitare sulla rete Internet)[25], sia normali comunicazioni tra presenti, effettuate senza l'ausilio di strumenti di trasmissione a distanza del suono o dell'immagine.

In realtà la legge processuale italiana regola le attività di intercettazione senza mai spiegare esattamente in che cosa esse consistano. A ritagliare i contorni del *genus* hanno dovuto provvedere gli interpreti: secondo una definizione comunemente accolta, costituisce intercettazione «la captazione occulta e contestuale di una comunicazione o conversazione tra due o più soggetti che agiscano con l'intenzione di escludere gli altri e con modalità oggettivamente idonee allo scopo, attuata da un soggetto estraneo alla stessa mediante strumenti tecnici di percezione tali da vanificare le cautele ordinariamente poste a protezione del suo carattere riservato»[26].

Non c'è dubbio che in questa generica fattispecie possa oggi farsi rientrare anche la captazione effettuata per il tramite del dispositivo elettronico informaticamente modificato. Con specifico riferimento alle intercettazioni di colloqui tra persone presenti, non bisogna però dimenticare che la materia è stata regolata in un momento storico nel quale gli inquirenti disponevano di strumenti di intercettazione (microspie, microfoni direzionali ecc.) dalle potenzialità intrusive infinitamente

---

[25] L'utilizzo del captatore informatico permette, in questi casi, di superare in radice i problemi legati alla protezione del sistema VOIP con tecniche di crittografia del tipo *end-to-end*, dal momento che il *trojan* «consente di intercettare la voce dell'utente prima che il segnale audio venga codificato dal protocollo di comunicazione criptato» (così CAJANI, Francesco. Odissea del captatore informatico, cit., p. 4143 s.). Sulla discussa applicabilità dell'art. 266 c.p.p. (intercettazioni di comunicazioni telefoniche o di altre forme di telecomunicazioni) o dell'art. 266-*bis* c.p.p. (intercettazioni di comunicazioni informatiche o telematiche) alle intercettazioni di comunicazioni vocali in transito sui circuiti VOIP cfr., anche per ulteriori riferimenti, lo stesso CAJANI, Francesco. *ivi*, p. 4143 s.

[26] Cass., Sez. un., 28 maggio 2003, Torcasio, *Cassazione penale*, 2004, p. 2094.

minori di quelle che possono oggi vantare uno *smartphone* o un *tablet* controllati a distanza. Certamente i codificatori del 1988 non potevano immaginare che a veicolare le comunicazioni e le immagini riservate sarebbe stato un oggetto in possesso della stessa persona intercettata, destinato ad accompagnare quest'ultima pressoché in ogni momento – e in ogni luogo[27] – della sua vita quotidiana. Nè potevano immaginare che gli inquirenti, alle condizioni tutt'altro che rigorose stabilite dagli artt. 266-271 c.p.p., avrebbero potuto agevolmente monitorare l'intera vita di relazione di una persona.

Ne derivano due considerazioni alquanto ovvie. La prima è che la vigente disciplina delle intercettazioni (e segnatamente, dell'intercettazione di comunicazioni tra presenti) nasce da una ponderazione degli interessi in gioco che non è più attuale. Nel delineare i "casi", i "modi" e le "garanzie" dell'intercettazione, e nel bilanciare le esigenze di investigazione penale con la salvaguardia del diritto alla segretezza delle comunicazioni e del diritto all'intimità domiciliare, il legislatore del 1988 non poteva mettere nel conto i gravi attentati alla *privacy* che si sarebbero consumati nell'epoca della *smartphone addiction* e dei cavalli di Troia informatici[28]. Ciò rende necessaria un'attenta rivalutazione normativa dei sacrifici imposti ai diritti individuali coinvolti, nel rispetto del principio di proporzione[29] e del parametro della «necessità in una

---

[27] Basti pensare, come rileva Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 20, che «il soggetto intercettato può recarsi, portando con sé l'apparecchio elettronico nel quale è stato installato il "captatore", nei luoghi di privata dimora di altre persone, così dando luogo ad una pluralità di intercettazioni domiciliari».

[28] Lo riconosce, in fondo, la stessa Cass., Sez. un., 28 aprile 2016, Scurato, cit., pp. 20, 22. Nel consentire l'uso dei captatori informatici come strumento di intercettazione – sia pure, ad avviso della Corte, nei soli procedimenti per delitti di criminalità organizzata (v. *infra*, § 5) –, il legislatore avrebbe operato «un accurato contemperamento di valori ed interessi», calibrando la notevole «compressione dei diritti fondamentali delle persone [che deriva dall'uso di tali strumenti di indagine] con l'efficace tutela delle esigenze dei singoli e della collettività in relazione a reati di particolare gravità». Ma questo «accurato contemperamento» degli interessi in gioco è avvenuto, ammettono le Sezioni unite, «*in un contesto temporale in cui la tecnologia non aveva ancora raggiunto l'attuale livello di efficacia e di capacità intrusiva*».

[29] Sul principio di proporzionalità come «fondamentale condizione di legittimità», specie in ambito eurounitario, «dei mezzi prescelti per ogni inter-

società democratica» richiesto dall'art. 8 della Convenzione europea dei diritti dell'uomo per qualunque attentato alla vita privata e familiare dell'individuo.

La seconda considerazione è che il *deficit* di determinatezza del paradigma intercettivo – e in particolare, il fatto che manchi nella disciplina codicistica qualunque riferimento alla tipologia degli strumenti di captazione – appare sempre meno tollerabile in una materia coperta da riserva di legge circa i "modi" e le "garanzie" dell'atto di indiscrezione visiva e acustica[30]. Il legislatore poteva dare per scontato che cosa fosse e come potesse venire effettuata un'intercettazione di comunicazioni tra presenti quando lo strumentario a disposizione degli inquirenti si riduceva alla microspia o al registratore da posizionare nel luogo in cui si ipotizzava che si sarebbe svolto il colloquio da intercettare. Ma è difficile ammettere che possa ancora farlo oggi, in presenza di modalità

vento pubblico nella sfera della libertà personale, intercettazioni incluse», cfr. LASAGNI, Giulia. L'uso di captatori informatici, cit., p. 20 s. Significative indicazioni si traggono, al riguardo, dalla già citata sentenza costituzionale tedesca del 20 aprile 2016 (v. *supra*, nota 17), concernente proprio indagini condotte con l'ausilio del *virus trojan*: poiché «il bilanciamento dei contrapposti valori costituzionali va condotto in forza del principio di proporzionalità», non solo «i poteri investigativi che incidono in maniera profonda sulla vita privata [vanno] limitati dalla legge alla tutela di interessi sufficientemente rilevanti nei casi in cui sia prevedibile un pericolo sufficientemente specifico a detti interessi», ma il «nucleo profondo della vita privata [deve essere] rigorosamente preservato per mezzo di norme particolari che innalzino il livello di garanzie», e il coinvolgimento di terzi estranei nell'attività investigativa può ritenersi consentito solo in «condizioni particolari».

30 Anche i requisiti qualitativi che la Corte europea dei diritti dell'uomo pretende siano rispettati nelle legislazioni nazionali nel disciplinare l'intercettazione di comunicazioni – il contenuto «sufficientemente chiaro e dettagliato» della disciplina, in grado di «offrire ai cittadini un'indicazione adeguata in ordine alle circostanze nelle quali l'autorità pubblica ha il potere di ricorrere a tali misure», anche con riferimento ai «potenziali destinatari delle intercettazioni» e ai luoghi da sorvegliare elettronicamente (cfr. Corte europea dei diritti dell'uomo, 10 febbraio 2009, Iordachi e altri c. Moldavia, e Corte europea dei diritti dell'uomo, 4 dicembre 2015, Zacharov c. Russia) – si direbbero ormai fare difetto. Per due diverse opinioni, al riguardo, cfr. FILIPPI, Leonardo. L'ispe-perqui-intercettazione "itinerante", cit., p. 4 s., e Procura Generale presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni unite*, cit., p. 16 s.

diversificate – e assai diversamente aggressive – di attacco alla sfera comunicativa riservata[31].

In sintesi, una presa di posizione normativa non appare più procrastinabile. Lacunosa e tecnicamente obsoleta, l'attuale disciplina delle intercettazioni si presta a letture evolutive che la rendono inconciliabile con il dettato costituzionale[32].

5. Non previsto e non prevedibile dal legislatore del 1988, l'uso dei dispositivi elettronici privati come strumento di intercettazione ha

---

[31] *Contra* LASAGNI, Giulia. L'uso di captatori informatici, cit., p. 11 s. («il rispetto della doppia riserva di legge e di giurisdizione richiesta dalla Costituzione per ogni tipo di intrusione nelle libertà fondamentali poste a tutela del domicilio privato e delle comunicazioni non si estende – nel quadro normativo vigente – anche alla necessità di avere una specifica previsione legislativa per ogni tipologia di strumento captativo utilizzabile»), sul presupposto che la disciplina delle intrusioni tecnologiche nella sfera privata sarebbe tendenzialmente indifferente al tipo di tecnologia utilizzata, come dimostrato anche dai principi ispiratori della nuova normativa europea in materia di protezione dei dati personali (Direttiva UE 2016/280 del Parlamento Europeo e del Consiglio del 27 aprile 2016, *Protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati*). Secondo l'Autrice, «sarebbe quindi auspicabile un intervento legislativo che identificasse chiaramente non tanto tutte le singole tecnologie utilizzabili nel campo delle intercettazioni (che prima erano microspie, oggi sono *virus* informatici, ma potrebbero ovviamente a breve avere anche forma ben diversa), quanto piuttosto *le garanzie fondamentali* che devono essere sempre riconosciute all'indagato e ai terzi potenzialmente coinvolti, *a prescindere dallo strumento utilizzato*» (*ivi*, 13, corsivo aggiunto). Il problema è che al variare delle tecniche intrusive si accompagna (come in definitiva riconosce la stessa Autrice, *ivi*, 20 ss.) la necessaria previsione di *specifiche* garanzie. Si pensi, per fare un solo esempio, alla necessità di evitare che il *malware* determini un abbassamento del livello di sicurezza del dispositivo su cui viene usato, o alla necessità di garantirne la disinstallazione a intercettazione conclusa (*v. infra*, § 6). Ciò rende comunque necessario l'aggiornamento legislativo della disciplina dell'intercettazione, con buona pace del principio di "neutralità tecnica" di tale disciplina.

[32] Per analoghe considerazioni si veda il documento redatto nel luglio 2016 da un gruppo di studiosi di Diritto processuale penale dell'Università di Torino, successivamente sottoscritto da più di settanta docenti universitari di Diritto, reperibile in <http://www.dg.unito.it/do/forms.pl/FillOut?_id=goux>. Ultimo accesso: 2 aprile 2017.

fatto sorgere inoltre uno specifico problema, del quale hanno dovuto occuparsi recentemente le Sezioni unite della Corte di cassazione.

L'art. 267 del codice italiano di procedura penale assoggetta le intercettazioni di comunicazioni tra presenti a condizioni diverse a seconda del luogo in cui la comunicazione si svolge. Per le comunicazioni effettuate al di fuori del domicilio occorrono i medesimi presupposti formali e sostanziali necessari per procedere alle intercettazioni telefoniche: devono sussistere "gravi indizi" di uno dei reati elencati nell'art. 266 c.p.p.; l'intercettazione deve risultare "assolutamente indispensabile ai fini della prosecuzione delle indagini"; occorre l'autorizzazione preventiva del giudice (salvi i casi di urgenza, nei quali l'intercettazione può essere disposta dal pubblico ministero con apposito decreto, che va tuttavia convalidato dal giudice nelle quarantotto ore successive). Per le comunicazioni tra presenti che si svolgono nei contesti domiciliari indicati dall'art. 614 c.p. – ossia «nell'abitazione, in un altro luogo di privata dimora o nelle appartenenze di essi» – è invece richiesta una rigorosa condizione supplementare: l'intercettazione «è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa» (art. 266 comma 2 c.p.p.). In altre parole, perché gli inquirenti possano installare una microspia all'interno di un'abitazione privata occorre che all'interno di quell'abitazione si stia presumibilmente commettendo il reato: non basta che vi sia fondato motivo di ritenere che vi si terranno conversazioni concernenti un reato già commesso.

L'applicazione di questa regola diventa tuttavia problematica quando lo strumento di intercettazione, anziché fisso come una tradizionale microspia, diventa mobile: ossia quando gli operatori – come accade inevitabilmente nell'ipotesi del dispositivo privato portatile – non sono in grado di conoscere in anticipo gli spostamenti dello strumento di captazione. Anche ad ammettere, infatti, che il microfono e la *webcam* del dispositivo bersaglio possano essere attivati e disattivati in qualunque momento nel corso delle operazioni investigative, rimane elevato il rischio che nella rete degli inquirenti finiscano comunicazioni non legittimamente intercettabili perché svolgentisi in un contesto domiciliare nel quale non si stanno commettendo reati.

L'esistenza di un simile rischio ha indotto le Sezioni unite della Corte di cassazione a ritenere che l'intercettazione di comunicazioni

tra persone presenti *non possa venire effettuata mediante l'impiego di captatori informatici*: o meglio, che ciò sia consentito solo nei casi eccezionali in cui la legge autorizza l'intercettazione domiciliare anche in assenza dello svolgimento attuale di un'attività criminosa, ossia nei casi in cui si proceda per delitti di "criminalità organizzata" (art. 13 comma 1 del d.l. n. 152 del 1991)[33]. La disciplina dell'intercettazione di colloqui *inter praesentes*, hanno stabilito le Sezioni unite, non è fisiologicamente incompatibile con il ricorso a dispositivi mobili[34]: ma poiché «all'atto

[33] Questo il principio di diritto enunciato da Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 23: «l'intercettazione di conversazioni o comunicazioni tra presenti – mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad es., *personal computer*, *tablet*, *smartphone*, ecc.) – [...] *è consentita* [...] 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 [...] *limitatamente ai procedimenti per delitti di criminalità organizzata*».

[34] Di avviso contrario Cass., Sez. VI, 26 maggio 2015, Musumeci, <www.italgiure.giustizia.it.>, Massime penali Corte Cassazione, n. 265654. Ultimo accesso: 8 aprile 2017, secondo cui, nell'autorizzare l'intercettazione di colloqui tra persone presenti (ovvero, come si usa dire, nel disporre intercettazioni "ambientali"), il giudice dovrebbe necessariamente indicare anche lo specifico luogo (l'"ambiente") in cui si svolgerà l'attività investigativa: indicazione che sarebbe impossibile da fornire quando lo strumento captativo sia "itinerante". Nello stesso senso, in dottrina, FILIPPI, Leonardo. L'ispe-perqui-intercettazione "itinerante", cit., p. 3, e LORENZETTO, Elisa. Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico", <www.penalecontemporaneo.it>, 24 marzo 2016, p. 2. Ultimo accesso: 6 aprile 2017. A giudizio delle Sezioni unite, invece, «il riferimento al luogo non integra un presupposto dell'autorizzazione», dal momento che la legge processuale allude all'intercettazione di comunicazioni tra persone presenti e non al monitoraggio di "ambienti" di alcun tipo; «non è dato rinvenire nelle vigenti disposizioni alcun accenno ad "intercettazioni ambientali", locuzione, questa, utilizzata generalmente nella giurisprudenza e in dottrina, [ed] entrata a far parte del linguaggio giuridico in un momento storico nel quale le possibilità di intercettazione in luoghi chiusi – in base alle tecniche di captazione disponibili – erano per lo più riconducibili alla installazione di microspie in uno o più "ambienti" predeterminati»; «per tale motivo – ed a maggior ragione perché una siffatta dizione non trova riscontro nel dato testuale delle norme di interesse – sarebbe errato giungere al punto da ritenere illegittima qualunque intercettazione tra presenti non strettamente collegata a un predeterminato "ambiente"». Di regola, pertanto, «deve ritenersi sufficiente che il decreto autorizzativo indichi il destinatario della captazione e la tipologia di ambienti dove essa va eseguita», ma «l'intercettazione resta utilizzabile anche qualora venga effettuata in un

di autorizzare un'intercettazione da effettuarsi a mezzo di captatore informatico installato su un apparecchio portatile, il giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto», non può nemmeno «effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale»; dunque, «si correrebbe il concreto rischio di dar vita ad una pluralità di intercettazioni tra presenti in luoghi di privata dimora del tutto al di fuori dei cogenti limiti previsti dalla vigente normativa codicistica». E «anche se fosse tecnicamente possibile seguire gli spostamenti dell'utilizzatore del dispositivo elettronico e sospendere la captazione nel caso di ingresso in un luogo di privata dimora, sarebbe comunque impedito il controllo del giudice nel momento dell'autorizzazione, che verrebbe disposta "al buio"»[35], rimanendo affidato agli inquirenti il compito di stabilire, volta per volta, se un determinato luogo rientri o meno nel paradigma evocato dall'art. 614 c.p.[36].

---

altro luogo rientrante nella medesima categoria» (Cass., Sez. un., 28 aprile 2016, Scurato, cit., pp. 14, 17, 19).

[35] Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 14 s.

[36] E' stato rilevato che il ragionamento della Corte sembra trascurare l'ipotesi in cui il giudice, in un procedimento per reati diversi da quelli di criminalità organizzata, abbia diligentemente indicato nel decreto autorizzativo il luogo di privata dimora da monitorare o la tipologia degli ambienti extradomiciliari nei quali potrà svolgersi l'intercettazione (v. *supra*, nota 34: ad esempio, "i bar frequentati dall'indagato"), prescrivendo espressamente che il microfono o la *webcam* siano attivati solo quando il dispositivo infettato viene introdotto in tali luoghi. In simili evenienze, il giudice non autorizzerebbe affatto "al buio" l'intercettazione, che dovrebbe ritenersi, pertanto, «pienamente legittima» (CAJANI, Francesco. Odissea del captatore informatico, cit., p. 4149 s.). Questa lettura della sentenza ha il merito di tracciare le coordinate all'interno delle quali dovrà muoversi – e si sta effettivamente muovendo (v. *infra*, § 6) – il legislatore nel regolare la materia: a) rendere più stringenti gli obblighi motivazionali del giudice, tipizzando le prescrizioni che dovranno essere contenute nel decreto autorizzativo; b) vietare espressamente l'utilizzo dei captatori informatici in grado di attivare il microfono e la *webcam* per effetto del solo inserimento nel dispositivo anziché di un apposito comando a distanza; c) garantire il rispetto delle condizioni poste dal giudice con adeguati accorgimenti tecnici, che rendano smascherabili a posteriori gli eventuali impieghi non autorizzati dello strumento di captazione.

All'enunciazione di questi principi, di indubbia portata garantistica, la Corte di cassazione affianca un'importante ulteriore precisazione.

Ritenere precluso *tout court* il ricorso al captatore informatico come strumento di intercettazione di comunicazioni tra presenti (salvo, come detto, che si proceda per delitti di criminalità organizzata) significa rinunciare a priori anche a possibili acquisizioni probatorie – le intercettazioni di colloqui extradomiciliari – che sarebbero del tutto legittime. Le Sezioni unite avrebbero dunque potuto optare per una diversa soluzione: consentire l'impiego del captatore informatico, invitando il giudice a distinguere, a posteriori, le intercettazioni effettuate fuori del domicilio, utilizzabili come prova, e quelle effettuate nel domicilio, vietate dalla legge e dunque inutilizzabili[37].

Si tratta dell'impostazione che la Corte di cassazione ha finora seguito in una fattispecie affine a quella in esame. Nel silenzio della legge processuale, ci si era chiesti se fosse consentito intercettare comunicazioni domiciliari tra presenti, nei casi previsti dall'art. 266 comma 2 c.p.p., *anche per mezzo di strumenti di ripresa visiva* (ossia di telecamere) anziché dei tradizionali strumenti di ripresa sonora. Il dubbio era nato perché in questo modo le telecamere finiscono inevitabilmente per riprendere anche comportamenti domiciliari di tipo non comunicativo, ossia per realizzare una violazione sensoriale del domicilio non regolata dalla legge, in contrasto con l'art. 14 Cost. Ciò nonostante, la Corte ha risposto affermativamente al quesito: ma precisando che il giudice, a posteriori, avrebbe dovuto accuratamente distinguere le riprese visive di comportamenti domiciliari comunicativi (consentite nel rispetto dei presupposti di cui agli artt. 266 comma 2 e 267 c.p.p., perché riconducibili al paradigma dell'intercettazione) e le riprese visive di comportamenti domiciliari non comunicativi (non regolate dalla legge, e, come tali, destinate a consegnare materiali cognitivi non utilizzabili in giudizio, in virtù di una regola di esclusione probatoria desumibile dallo

[37] Era questa la soluzione prospettata dalla Sesta Sezione nell'ordinanza di rimessione alle Sezioni unite (cfr. Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 14 s.: «il controllo non potrà che essere successivo e riguardare il regime dell'inutilizzabilità delle conversazioni captate in uno dei luoghi indicati dall'art. 614 c.p.»).

stesso art. 14 Cost.)[38]. La replica della dottrina era stata immediata: l'*home-watching* abusivo non avrebbe potuto certamente ritenersi scriminato per il solo fatto di produrre materiali audiovisivi non spendibili in giudizio (tanto più ove il titolare del diritto violato fosse un soggetto del tutto disinteressato alle sorti dell'inchiesta penale). Di fatto, la Corte autorizzava gli inquirenti a perpetrare gravi violazioni del diritto all'intimità domiciliare non previste dalla legge[39].

La verità è che il rischio di incidere su diritti fondamentali dell'individuo al di fuori dei confini tracciati dalla legge (costituzionale e ordinaria) è motivo sufficiente perché debbano ritenersi banditi dal processo penale gli strumenti investigativi le cui potenzialità intrusive non siano determinabili a priori[40], benché questo significhi privarsi anche delle legittime risultanze probatorie che simili strumenti potrebbero offrire[41].

Su queste posizioni più rigorose sembrerebbe essersi assestata la decisione delle Sezioni unite in materia di *virus* informatici. «Nel caso di captazioni eventualmente avvenute in luoghi di privata dimora al di fuori dei presupposti di cui all'art. 266 comma 2 c.p.p.», osservano i giudici della Cassazione, «*non potrebbe nemmeno invocarsi la sanzione della inutilizzabilità*»: sia perché si tratta di una sanzione processuale

---

[38] Per tutte Cass., Sez. IV, Besnik, <www.italgiure.giustizia.it.>, Massime penali Corte Cassazione, n. 231047. Ultimo accesso: 8 aprile 2017.

[39] Cfr., volendo, CAPRIOLI, Francesco. Riprese visive nel domicilio, cit., p. 2203 s., e Id., Nuovamente al vaglio della Corte costtuzionale l'uso investigativo degli strumenti di ripresa visiva, *Giurisprudenza costituzionale*, 2008, p. 1839 s. Più di recente, nel senso che «resta insuperabile il dato oggettivo della tardività del rimedio rispetto alla tutela effettiva del diritto alla inviolabilità del domicilio», in quanto «la sanzione processuale dell'inutilizzabilità delle immagini non comunicative può logicamente intervenire soltanto *a posteriori*, e cioè a lesione della libertà ormai avvenuta», cfr. DEL COCO, Rosita. *In*: SCALFATI, Adolfo (a cura di). Registrazioni audio-video su impulso dell'investigatore. *Le indagini atipiche*, cit., p. 27.

[40] Come un dispositivo portatile infettato da un *malware*, i cui movimenti nello spazio non sono preventivabili: ma anche come una videocamera installata in un domicilio, che non si può sapere a priori se riprenderà solo comportamenti comunicativi o anche comportamenti non comunicativi.

[41] Vale a dire, nel caso dei *trojans*, le intercettazioni di colloqui extradomiciliari, e, nel caso delle riprese video domiciliari, le captazioni riconducibili al *genus* dell'intercettazione perché aventi ad oggetto comportamenti comunicativi.

«riservata a gravi patologie degli atti del procedimento e del processo, e non ad ipotesi di adozione di provvedimenti *contra legem* e non preventivamente controllabili quanto alla loro conformità alla legge», sia, soprattutto, perché si tratta di una sanzione che opererebbe tardivamente, quando gravi lesioni non autorizzate dei diritti di *privacy* si sono già interamente consumate (essendo, in particolare, «concreto il rischio della possibile divulgazione, ben prima di ogni declaratoria di inutilizzabilità, dei contenuti di intercettazioni destinate ad essere successivamente dichiarate inutilizzabili»)[42].

E' un'impostazione certamente condivisibile[43]: l'auspicio è che questa nuova consapevolezza induca i giudici di legittimità a rivedere anche le opinioni espresse in materia di videoriprese domiciliari[44].

---

[42] Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 15, in linea con le considerazioni svolte dalla Procura Generale presso la Corte di cassazione nella memoria per la camera di consiglio (cit., p. 21). Definisce questa, giustamente, «la scelta profonda della sentenza Scurato», GIORDANO, Luigi. Dopo le Sezioni Unite sul "captatore informatico", cit., p. 9 s.

[43] In un passaggio della motivazione (Cass., Sez. un., 28 aprile 2016, Scurato, cit., p. 21), le Sezioni unite sembrerebbero in verità ricadere nell'impostazione precedentemente ripudiata. «Per quel che riguarda l'eventualità che lo strumento captativo in argomento possa produrre, in casi estremi, esiti lesivi della dignità umana» – rileva la Corte, riferendosi al possibile impiego dei *virus* informatici nei procedimenti per delitti di criminalità organizzata – «va osservato, come opportunamente prospettato dai rappresentanti della Procura generale nella memoria in atti, che si tratta di un pericolo che ben può essere neutralizzato con gli strumenti di cui dispone l'ordinamento; ad esempio, "facendo discendere dal principio personalistico enunciato dall'art. 2 della Costituzione, e dalla tutela della dignità della persona che ne deriva, la sanzione di inutilizzabilità delle risultanze di 'specifiche' intercettazioni che nelle loro modalità di attuazione e/o nei loro esiti abbiano acquisito 'in concreto' connotati direttamente lesivi della persona e della sua dignità"» (Procura Generale presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni unite*, cit., p. 18). Come se, ancora una volta, l'inutilizzabilità processuale bastasse a rendere innocua – e costituzionalmente tollerabile – un'attività investigativa atipica lesiva della dignità umana.

[44] Come già accennato, anche una videoripresa (domiciliare o extradomiciliare) può oggi essere effettuata per mezzo di un *virus trojan* installato su un dispositivo elettronico. Nel caso esaminato dalla sentenza delle Sezioni unite, tuttavia, il giudice per le indagini preliminari aveva espressamente negato l'autorizzazione all'utilizzo del captatore per l'effettuazione di videoriprese (Procura Generale presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni unite*, cit., p. 10).

6. Qualche cenno conclusivo va riservato ai progetti di riforma concernenti la materia in esame. Due, fra le altre[45], le iniziative da menzionare.

La prima è la proposta di legge C. 4260 (primo firmatario l'on. Quintarelli), depositata alla Camera dei deputati il 31 gennaio 2017[46], che contiene una dettagliata disciplina di tre diverse attività investigative realizzabili per mezzo del "captatore informatico": 1) la «osservazione e acquisizione da remoto» (più specificamente, la «osservazione dei dispositivi» e la «acquisizione da remoto dei dati contenuti in un sistema informatico o telematico, diversi da quelli relativi al traffico telefonico o telematico»); 2) la «intercettazione di conversazioni e comunicazioni, anche tra presenti»[47]; 3) la «acquisizione della posizione geografica della persona sottoposta alle indagini».

L'uso del *trojan horse* informatico viene consentito nei soli procedimenti per reati di criminalità organizzata di stampo mafioso o con finalità di terrorismo (artt. 254-*ter* comma 1, 266-*bis* comma 1-*bis*, 266-*ter* comma 1 c.p.p.)[48]. Si stabilisce, inoltre, che le indagini del primo e del se-

---

[45] 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, si era ipotizzato di modificare l'art. 266-*bis* c.p.p. (che regola l'intercettazione «del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi») 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». In seguito, si era proposto di limitare l'utilizzo del nuovo strumento investigativo alle sole indagini per i delitti di cui agli artt. 270-*bis*, 270-*ter*, 270-*quater* e 270-*quinquies* c.p., commessi con le finalità di terrorismo di cui all'art. 270-*sexies* c.p. Una proposta analoga era contenuta nella proposta di legge C. 3470 depositata in data 2 dicembre 2015 alla Camera dei Deputati (*Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche*).

[46] V. *supra*, nota 1.

[47] Ivi compresi «i flussi di comunicazioni [che] risultino cifrati, in tutto o in parte» (art. 266-*bis* comma 1-*ter* c.p.p.).

[48] Come si legge nella Relazione alla proposta, «è evidente che vi sono altre tipologie di reati molto gravi, che destano ribrezzo e sdegno sociale, per contrastare i quali l'utilizzo del captatore può offrire grandi possibilità, primo tra tutti la pedopornografia. Tuttavia si tratta di un punto di equilibrio con i diritti costituzionali di assai difficile individuazione; la definizione del perimetro

condo tipo possano venire effettuate solo quando non sia «possibile distinguere un ambito di attività o di vita personale estraneo all'associazione criminale» (art. 254-*ter* comma 1 c.p.p.), ovvero quando «l'effettiva natura dell'organizzazione criminale [...] presenti connotati di pervasività tali da [...] ostacolare una separazione tra attività illecita e ordinaria vita privata» (artt. 254-*ter* comma 2, 266-*bis* comma 1-*quater* c.p.p.). L'osservazione e l'acquisizione da remoto potranno essere disposte[49] alle stesse condizioni già previste dalla legge italiana per l'intercettazione di comunicazioni: vale a dire, solo «dal giudice su richiesta del pubblico ministero»[50], e solo «quando vi [sia]no gravi indizi di reato» e l'atto investigativo risulti «assolutamente indispensabile per la prosecuzione delle indagini» (art. 254-*ter* comma 1 c.p.p.). Nel decreto autorizzativo del giudice andranno «indicati i dispositivi sui quali può essere effettuata l'installazione» dei programmi o strumenti informatici utilizzati, con l'esposizione dettagliata dei motivi per i quali si è resa eventualmente «necessaria l'installazione su dispositivi di soggetti non indagati» (art. 268-*bis* comma 4 c.p.p.). Il pubblico ministero potrà delegare le attività investigative svolte a mezzo di captatori informatici «soltanto alla polizia giudiziaria», che non potrà «avvalersi di ausiliari» (art. 268-*bis* comma 6 c.p.p.)[51]. Tali attività andranno comunque effettuate «sempre nel rispet-

di applicabilità è quindi un tema estremamente delicato. In questa proposta di legge, oltre a definire con cura le garanzie delle parti e del procedimento, i proponenti hanno ritenuto opportuno limitare il perimetro dell'utilizzabilità ai soli reati che attentano all'integrità dello Stato. Sarà un'approfondita riflessione nel Parlamento, sede del processo democratico, a stabilire il perimetro di utilizzabilità più appropriato». Con specifico riferimento all'intercettazione di comunicazioni tra presenti, si fa notare, in ogni caso, come la previsione di questo limite si ponga «in continuità con quanto stabilito dalla Corte di cassazione» nella sentenza Scurato.

49 Per quaranta giorni, prorogabili più volte, fino a un massimo di dodici mesi, nel caso in cui l'interruzione delle operazioni (seguita dalla notifica del decreto autorizzativo all'interessato) provocherebbe un «grave pregiudizio alle indagini»: art. 254-*ter* comma 3 c.p.p.

50 Come già sappiamo (*supra*, § 3), per i firmatari della proposta le perquisizioni *online* violano il domicilio informatico: di qui il necessario coinvolgimento dell'organo giurisdizionale nella procedura autorizzativa.

51 «Tale previsione è fondamentale per circoscrivere l'ambito di utilizzo dello strumento investigativo e dei relativi atti di indagine, anche in considerazione dell'impossibilità per le forze di polizia e per la magistratura di verificare

to della dignità umana e personale e, nei limiti del possibile, nel rispetto del pudore e della riservatezza della sfera privata di chi vi è sottoposto» (artt. 254-*ter* comma 2, 266-*bis* comma 1-*quinquies* c.p.p.)[52].

Gli strumenti e i programmi informatici utilizzati dovranno infine possedere «i requisiti stabiliti con regolamento adottato mediante decreto del Ministro della Giustizia, di concerto con il Ministro dell'Interno e su parere conforme del Garante per la Protezione dei dati personali» (art. 268-*bis* comma 8 c.p.p.)[53]: al termine dell'attività investigati-

---

l'operato di un tale soggetto (non ufficiale di polizia giudiziaria ma mero tecnico informatico) che opera distante dai loro occhi e dai loro uffici e spesso per mezzo di apparati telematici non verificabili e in *cloud*» (così la Relazione alla proposta di legge).

[52] «Con questa previsione si intende ribadire che la captazione da remoto di conversazioni, un potente e talvolta insostituibile strumento di indagine, non può svolgersi con modalità tali da sacrificare il principio personalista, pietra angolare del nostro ordinamento costituzionale, il cui rispetto deve prevalere sullo stesso interesse pubblico alla repressione dei reati» (così ancora la Relazione alla proposta di legge).

[53] Di grande interesse, a questo riguardo, i contenuti del progettato art. 89-*bis* delle norme di attuazione, coordinamento e transitorie del codice di procedura penale (art. 6 della proposta): «il regolamento del Ministro della giustizia di cui all'art. 268-*bis* comma 8 del codice, da aggiornare almeno ogni tre anni, stabilisce i requisiti tecnici che gli strumenti o programmi informatici devono possedere per garantire che la loro installazione e attivazione per l'osservazione e l'acquisizione di dati da remoto non alterino i dati stessi né le restanti funzioni del dispositivo ospite; disciplina altresì le modalità con le quali deve essere assicurata la conformità del programma o strumento informatico utilizzato ai predetti requisiti nonché le relative procedure di utilizzo e aggiornamento e reca le specifiche di dettaglio relative all'utilizzo e all'aggiornamento del programma o strumento, sulla base dei seguenti criteri direttivi: (a) istituzione di un sistema di omologazione, affidato all'Istituto Superiore delle comunicazioni e delle tecnologie dell'informazione, dei programmi e strumenti informatici utilizzabili ai sensi degli artt. 266-*bis*, 266-*ter* e 254-*ter* del codice. L'omologazione deve essere ripetuta almeno ogni dodici mesi per garantire la validità di tutte le edizioni dei captatori intermedie rilasciate come aggiornamento dell'edizione già omologata; (b) introduzione di un obbligo di deposito dei codici sorgenti, presso un ente da determinare, con una procedura tale da garantire a posteriori la ripetibilità indipendente del processo di omologazione di una specifica edizione del programma o strumento informatico, riproducendo l'esatta copia del programma o strumento utilizzato in fase di indagine a partire dai suoi codici sorgenti e di tutte le sue edizioni intermedie instanziate o installate, qualora l'impronta identificativa sia differente. Il deposito dei codici sorgenti deve essere effettuato per

ogni singola edizione di *software* rilasciato dai produttori almeno ogni dodici mesi; (c) introduzione di una garanzia di rintracciabilità del programma o strumento informatico utilizzato, tale da consentire alle parti di validarne la legittimità a posteriori, istituendo una base di dati apposita, il Registro nazionale dei captatori informatici, che raccoglie in tempo reale e con garanzia di integrità dei dati nonché validità temporale tutte le impronte digitali di tutte le edizioni di captatori informatici omologati rilasciati dai produttori e installate sui dispositivi obiettivo di indagine. Il Registro è gestito dall'ente di omologazione che lo mette a disposizione delle Forze di pubblica sicurezza, dei servizi di informazione e dei difensori delle parti direttamente interessate dall'intrusione informatica. Le richieste di informazioni, possibili solo da parte degli avvocati difensori di indagati che sono stato oggetto di verifica tramite captatore, non hanno carattere di onerosità per i richiedenti e devono essere espletate entro trenta giorni dalla richiesta; (d) previsione di un obbligo di registrazione di tutte le operazioni svolte dal programma o strumento informatico, dalla sua installazione fino alla sua rimozione, messe integralmente a disposizione delle parti come allegato del fascicolo, in modo da garantire l'autenticità e l'integrità dei dati; (e) previsione del divieto, per il programma o strumento informatico, di determinare un abbassamento del livello di sicurezza del sistema o del dispositivo su cui viene usato. E' fatta eccezione esclusivamente per le eventuali fasi di installazione che richiedano un temporaneo abbassamento del livello di sicurezza del sistema o del dispositivo, che deve comunque essere riportato alla condizione originaria al termine della procedura di installazione, sia essa andata a buon fine o no; (f) previsione dell'obbligo, al termine dell'uso dei programmi o strumenti informatici, di provvedere alla loro disinstallazione e, qualora la rimozione non sia stata possibile, previsione della fornitura all'utente delle informazioni tecniche necessarie affinché egli vi possa provvedere autonomamente; (g) introduzione di un obbligo di messa a disposizione da parte dei produttori, pubblicamente e gratuitamente, degli strumenti *software*, necessari per l'analisi dell'allegato al fascicolo di cui alla lettera d), inclusivi delle relative documentazione tecnica e specificazione del formato dati. Tali strumenti devono abilitare le parti a verificare in modo indipendente il rispetto dei requisiti di integrità nonché della completezza dell'allegato al fascicolo di cui alla citata lettera d), ovvero validare che questo includa la registrazione di tutte le fasi di operatività del captatore, dalla generazione dell'istanza specifica, a tutte le azioni effettuate sino alla sua disinstallazione; (h) introduzione di un sistema che consenta alle parti di richiedere ed eseguire in modo indipendente la verifica del processo di omologazione. La procedura di verifica fornita dal produttore deve garantire a posteriori la ripetibilità del processo di omologazione di una specifica edizione del programma o strumento informatico, riproducendo l'esatta copia del programma o strumento utilizzato in fase di indagine a partire dai suoi codici sorgenti e di tutte le sue edizioni intermedie instanziate o installate. Il produttore deve fornire come prestazione obbligatoria remunerata, su richiesta delle parti coinvolte in un caso che veda l'utilizzo di un captatore da questi certificato, la messa a disposizione di personale

va, tali strumenti andranno obbligatoriamente «rimossi dal dispositivo in cui erano stati installati», operazione della quale dovrà essere «redatto verbale» (art. 268-*bis* comma 7 c.p.p.).

La seconda iniziativa di riforma che va ricordata è il disegno di legge n. 2067 (*Modifiche al codice penale, al codice di procedura penale e all'ordinamento penitenziario*), approvato con voto di fiducia in Senato il 15 marzo 2017 e attualmente all'esame della Camera dei Deputati.

L'art. 1 comma 82 del testo approvato in Senato attribuisce al Governo la delega ad adottare decreti legislativi per la riforma della disciplina delle intercettazioni, secondo i princìpi e criteri direttivi previsti dal comma 84. Con specifico riferimento alle «intercettazioni di comunicazioni o conversazioni tra presenti mediante immissione di captatori informatici in dispositivi elettronici portatili», è prescritto che l'attivazione del dispositivo dovrà essere sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51 commi 3-*bis* e 3-*quater* c.p.p.; negli altri casi, l'intercettazione domiciliare mediante il *trojan* è consentita solo se nel domicilio si sta svolgendo l'attività criminosa. Per evitare ingressi sensoriali non autorizzati nel domicilio, è stabilito che l'attivazione del microfono potrà avvenire «solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice». In ogni caso, tale decreto dovrà indicare le ragioni che rendono necessario per lo svolgimento delle indagini il ricorso al captatore informatico come strumento di intercettazione. Inoltre, i risultati dell'intercettazione potranno essere «utilizzati a fini di prova soltanto dei reati oggetto del provvedimento autorizzativo»[54], e non potranno essere «in alcun modo conoscibili, divulgabili e pubblicabili [quando] abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede»[55].

---

tecnico o la documentazione atta a spiegare il funzionamento del sistema. La tariffa che il produttore può stabilire non può essere superiore alla tariffa media praticata dai consulenti tecnici d'ufficio nei confronti delle procure della Repubblica per consulenze inerenti l'informatica forense».

[54] Sui rischi «di strumentalizzazione dell'addebito associativo» che la norma intende prevenire cfr. GIORDANO, Luigi. Dopo le Sezioni Unite sul "captatore informatico", cit., p. 7 s.

[55] Più nel dettaglio, i decreti legislativi dovranno prevedere che: «1) l'attivazione del microfono avvenga solo in conseguenza di apposito comando inviato da

Bibliografia

AMORTH, Antonio. *La costituzione italiana*. Milano: Giuffrè, 1948.

BRICOLA, Franco. Prospettive e limiti della tutela penale della riservatezza. *Rivista italiana diritto e procedura penale*, 1967, p. 1120 s.

CAJANI, Francesco. Odissea del captatore informatico. *Cassazione penale*, 2016, p. 4140 s.

---

remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto autorizzativo del giudice; 2) la registrazione audio venga avviata dalla polizia giudiziaria o dal personale incaricato ai sensi dell'articolo 348 comma 4 c.p.p., su indicazione della polizia giudiziaria operante che è tenuta a indicare l'ora di inizio e fine della registrazione, secondo circostanze da attestare nel verbale descrittivo delle modalità di effettuazione delle operazioni di cui all'art. 268 del medesimo codice; 3) l'attivazione del dispositivo sia sempre ammessa nel caso in cui si proceda per i delitti di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p.p. e, fuori da tali casi, nei luoghi di cui all'articolo 614 del codice penale soltanto qualora ivi si stia svolgendo l'attività criminosa, nel rispetto dei requisiti di cui all'articolo 266 comma 1 c.p.p.; in ogni caso il decreto autorizzativo del giudice deve indicare le ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini; 4) il trasferimento delle registrazioni sia effettuato soltanto verso il *server* della procura, così da garantire originalità e integrità delle registrazioni; al termine della registrazione il captatore informatico venga disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante; 5) siano utilizzati soltanto programmi informatici conformi a requisiti tecnici stabiliti con decreto ministeriale da emanare entro trenta giorni dalla data di entrata in vigore dei decreti legislativi di cui al presente comma, che tenga costantemente conto dell'evoluzione tecnica al fine di garantire che tali programmi si limitino ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia; 6) fermi restando i poteri del giudice nei casi ordinari, ove ricorrano concreti casi di urgenza, il pubblico ministero possa disporre le intercettazioni di cui alla presente lettera, limitatamente ai delitti di cui all'articolo 51, commi 3-*bis* e 3-*quater* c.p.p., con successiva convalida del giudice entro il termine massimo di quarantotto ore, sempre che il decreto d'urgenza dia conto delle specifiche situazioni di fatto che rendono impossibile la richiesta al giudice e delle ragioni per le quali tale specifica modalità di intercettazione sia necessaria per lo svolgimento delle indagini; 7) i risultati intercettativi così ottenuti possano essere utilizzati a fini di prova soltanto dei reati oggetto del provvedimento autorizzativo e possano essere utilizzati in procedimenti diversi a condizione che siano indispensabili per l'accertamento dei delitti di cui all'articolo 380 c.p.p.; 8) non possano essere in alcun modo conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede» (art. 1 comma 84 lett. *e*).

CAPRIOLI, Francesco. Riprese visive nel domicilio e intercettazione "per immagini". *Giurisprudenza costituzionale*, 2003, p. 2176 s.

CAPRIOLI, Francesco. Nuovamente al vaglio della Corte costituzionale l'uso investigativo degli strumenti di ripresa visiva. *Giurisprudenza costituzionale*, 2008, p. 1832 s.

CORDERO, Franco. *Procedura penale*. Milano: Giuffrè, 2003.

DEL COCO, Rosita. Registrazioni audio-video su impulso dell'investigatore. *In*: SCALFATI, Adolfo (a cura di), *Le indagini atipiche*. Torino: Giappichelli, 2014, p. 27 s.

DOCUMENTO REDATTO DAI DOCENTI TORINESI DI PROCEDURA PENALE SUL PROBLEMA DEI CAPTATORI INFORMATICI. Reperibile in: <http://www.dg.unito.it/do/forms.pl/FillOut?_id=goux>. Ultimo accesso: 2 aprile 2017.

FELICIONI, Paola. L'acquisizione da remoto di dati digitali nel procedimento penale: evoluzione giurisprudenziale e prospettive di riforma. *Processo penale e giustizia*, 2016, p. 118 s.

FILIPPI, Leonardo. L'ispe-perqui-intercettazione "itinerante": le Sezioni unite azzeccano la diagnosi, ma sbagliano la terapia. *Archivio penale (web)*, 2016, n. 2, p. 1 s.

GIORDANO, Luigi. Dopo le Sezioni Unite sul "captatore informatico": avanzano nuove questioni, ritorna il tema della funzione di garanzia del decreto autorizzativo. Reperibile in: <www.penalecontemporaneo.it>. Utimo accesso: 1 aprile 2017.

IOVENE, Federica. Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale. *Rivista trimestrale Diritto penale contemporaneo*, 2014, 3-4, p. 329 s.

LASAGNI, Giulia. L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti". Reperibile in: <www.penalecontemporaneo.it>. Ultimo accesso: 1 aprile 2017.

LORENZETTO, Elisa. Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico". Reperibile in: <www.penalecontemporaneo.it>. Ultimo accesso: 1 aprile 2017.

ORLANDI, Renzo. Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici. *Archivio pen*ale (bollettino web), 25 luglio 2016.

PROCURA Generale presso la Corte di Cassazione, *Memoria per la camera di consiglio delle Sezioni unite del 28 aprile 2016*. Reperibile in: <www.penalecontemporaneo.it>. Ultimo accesso: 2 aprile 2017.

TESTAGUZZA, Alessandra. I sistemi di controllo remoto: fra normativa e prassi. *Diritto penale e processo*, 2014, p. 759 s.

TROGU, Mauro. Sorveglianza e "perquisizioni" online su materiale informatico. *In*: SCALFATI, Adolfo (a cura di). *Le indagini atipiche*. Torino: Giappichelli, 2014, 444.

VENEGONI, Andrea; GIORDANO, Luigi. La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici. Reperibile in: <www.penalecontemporaneo.it>. Ultimo accesso: 1 aprile 2017.

DADOS DO PROCESSO EDITORIAL
(http://www.ibraspp.com.br/revista/index.php/RBDPP/about/editorialPolicies)

- Recebido em: 31/03/2017
- Controle preliminar e verificação de plágio: 01/04/2017
- Retorno rodada de correções: 02/04/2017
- Avaliação 1: 02/04/2017
- Avaliação 2: 14/04/2017
- Decisão editorial final: 15/04/2017

Equipe editorial envolvida
- Editor-chefe: 1 (VGV)
- Editor-associado: 1 (MMGV)
- Editora-assistente: 1 (BC)
- Revisores: 2

COMO CITAR ESTE ARTIGO:

CAPRIOLI, Francesco. Il "captatore informatico" come strumento di ricerca della prova in Italia. *Revista Brasileira de Direito Processual Penal*, Porto Alegre, vol. 3, n. 2, p. 483-510, mai./ago. 2017. https://doi.org/10.22197/rbdpp.v3i2.71