TERESA BENE

"Il re è nudo": anomie disapplicative a proposito del captatore informatico

Nonostante la riforma della disciplina delle intercettazioni si sia posta il problema della protezione della riservatezza, il nostro sistema non ha ancora trovato un equilibrio soddisfacente tra interessi costituzionalmente rilevanti. Nel lavoro si prospetta l'inadeguatezza della disciplina dell'atto tipico applicata alle caratteristiche ed alle funzionalità dei software disponibili ad usi intercettativi.

"The king is naked": anomalous disapplicative about the computer programmer

Although the reform of the regulation of wiretapping has raised the issue of protecting privacy, our system has not yet found a satisfactory balance between constitutionally relevant interests. In the work the inadequacy of the discipline of the typical act applied to the features and functionalities of the software available for intercepting purposes is envisaged.

1.*Evoluzioni tecnologiche dei software.* L'attuale dibattito sullo strumento investigativo noto come *trojan* sembra caratterizzato da una sorta di contraddizione. Da un lato, sono sempre più frequenti le voci che si levano per segnalare come l'uso dello strumento investigativo abbia assunto manifestazioni esorbitanti con conseguente pregiudizio recato agli interessi coinvolti. Dall'altro, non è contestabile la dipendenza cognitiva degli uffici di procura dal mezzo tecnologico intercettativo, per quanto qui di interesse. Di conseguenza appare necessario interrogarsi sul tema della disciplina dell'atto tipico e chiedersi se essa sia adeguata a sostenere la peculiare tecnologia del captatore informatico, ovvero se l'ineffettività delle norme vigenti potrebbe essere determinata dalla loro inadeguatezza strutturale. L'approccio alla complessità di profili embricati tra di loro non può trascurare, infatti, l'evoluzione tecnologica delle caratteristiche e delle funzionalità dei software disponibili a fini intercettativi. Il profilo pone quale tema centrale di un dibattito, già animato, il rapporto tra la sicurezza collettiva, che deve essere garantita dallo Stato, e il diritto alla riservatezza dell'individuo. Su altro fronte, inquieta che il legislatore si occupi con passo incerto, oggi del captatore informatico, mentre si fanno largo nuovi protocolli di comunicazione che presuppongono un bagaglio di conoscenze tecniche adeguate a offrire corrette soluzioni interpretative.
Con ciò non si vuol dire che le diverse criticità relative allo strumento di indagine abbiano trovato soluzione[1]. Gli interessi contrapposti sono molteplici e

[1] Si veda GIOSTRA, *I nuovi equilibri tra diritto alla riservatezza e diritto di cronaca nella riformata disciplina delle intercettazioni,* in *Riv. it. dir. proc. pen.*, 2018, 2, 521 e ss.; si veda altresì FURFARO, *Intercet-*

relativi sia alla sfera pubblica sia a quella privata. Tali interessi possono essere collocati lungo linee immaginarie: esigenze della giustizia, tutela della riservatezza e necessario bilanciamento in ossequio ai criteri di ragionevolezza e proporzionalità, indicati dalla Corte Edu, quali principi essenziali di una società democratica[2]. L'impressione è che la situazione di forte criticità sia determinata dalla difficoltà di bilanciare esigenze divergenti e tendenzialmente antinomiche, come emerge con forza dinanzi al quadro della realtà politico-giudiziaria che si è recentemente svelato anche agli occhi del grande pubblico, lasciando fuori fraintendimenti e funambolismi.

L'intento è di rilevare un profilo di crisi del sistema operativo del captatore informatico[3] che si proietta sul rischioso versante dei delicati rapporti tra pubblico ministero, polizia giudiziaria ed ausiliari e che, in assenza delle necessarie garanzie anche solo sul piano tecnico, realizza inaccettabili violazioni delle libertà dei cittadini. Rischi che appaiono ancor maggiori dopo che il legislatore ha esteso la straordinaria efficacia esplorativa e acquisitiva del captatore informatico ai procedimenti per i reati contro la pubblica amministrazione.

La legge-delega 23 giugno 2017, n. 103 e il d.lgs. 29 dicembre 2017, n. 216[4], seguendo la scia della sentenza Scurato, hanno disciplinato il captatore infor-

---

tazioni: il sistema, la riforma e l'Europa, in *questa Rivista*, spec. Riforme, 2018, 473- 495; GAITO – FURFARO, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *questa Rivista*, 2016, 2, 309- 330; GIUNCHEDI, *Appunti su alcune criticità della nuova disciplina sulle intercettazioni*, in *questa Rivista*, spec. Riforme, 2018, 513- 525.

[2] Corte edu, 29 marzo 2005, Matheron c. Francia; tra le altre: Corte edu, 24 agosto 1998, Lambert c. Francia; Corte EDU, 25 marzo 1983, Silver e altri c. Regno Unito; Corte EDU, 6 settembre 1978, Klass e altri c. Germania.

[3] Cfr. RIVELLO, *Le intercettazioni mediante captatore informatico*, in *Le nuove intercettazioni*, a cura di Mazza, Torino, 2018, 101 ss.; BONTEMPELLI, *Il captatore informatico in attesa della riforma*, in *www.penalecontemporaneo.it*; ORLANDI, *Usi investigativi dei cosiddetti captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, 544 ss.; SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra, Orlandi, Torino, 2018, 269 ss.

[4] La cui efficacia, relativamente ai profili qui di interesse, era originariamente differita ai provvedimenti autorizzativi emessi dopo il 31 luglio 2019, termini poi prorogato dal cd. decreto sicurezza *bis*, decreto-legge 14 giugno 2019, n. 53, convertito in l. 8 agosto 2019, n. 77, al 31 dicembre 2019. La disposizione transitoria del d.lgs. 216/2017, all'art. 9, prevedeva che «1. Le disposizioni di cui agli articoli 2, 3 4, 5 e 7 si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il centottantesimo giorno successivo alla data di entrata in vigore del presente decreto». Le disposizioni normative contenute nell'art. 1 (che ha introdotto l'art. 617 *septies* c.p., cioè il reato di diffusione di riprese e registrazioni fraudolente) e nell'art. 6 (che consente che, nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p., si applichi la disciplina speciale di cui all'art. 13 d.l. 13 maggio 1991, n. 152, conv., con mod., dalla l. 12 luglio 1991, n. 203), sono entrate in vigore alla decorrenza della ordinaria della *vacatio legis*. Diversamente, per le altre disposizioni (artt. 2-3-4-5-

matico, come è noto, esclusivamente quale modalità per le intercettazioni *inter praesentes*[5], escludendo le molteplici potenzialità dello strumento tecnologico e gli effetti, ad esempio, dell'uso del captatore per le attività di ispezione, perquisizione, sequestro[6].

---

7), il d.lgs. prevedeva un differimento dell'entrata in vigore, oltre la ordinaria *vacatio legis*, al 25 luglio 2018. Si stabiliva, invece, che acquistasse efficacia decorsi dodici mesi dalla data di entrata in vigore dello stesso decreto legislativo 216/2017, la disposizione di cui all'art. 2, co. 1, lettera b), circa la pubblicazione dell'ordinanza cautelare di cui all'art. 292 c.p.p. Del decreto legislativo sono , dunque, entrati in vigore, dopo la ordinaria *vacatio legis*, e cioè a partire dal 26 gennaio 2018, soltanto l'art. 1 (che ha introdotto l'art. 617 *septies* c.p., cioè il reato di diffusione di riprese e registrazioni fraudolente) e l'art. 6 (che consente che, nei procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata a norma dell'art. 4 c.p.p., si applichi la disciplina speciale di cui all'art. 13 d.l. 13 maggio 1991, n. 152, conv., con mod., dalla l. 12 luglio 1991, n. 203). Con il d.l. 91/2018, conv. dalla l. n. 108/2018, c.d. "decreto milleproroghe", è stato previsto un primo slittamento al 31 marzo 2019 delle disposizioni di cui agli artt. 2, 3, 4, 5 e 7 del d.lgs. n. 216/2017. La legge di bilancio, 30 dicembre 2018, n. 145 ha spostato in avanti di ulteriori 4 mesi l'entrata in vigore della riforma stabilendo che le nuove disposizioni si applicano alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019, mentre la pubblicazione dell'ordinanza cautelare è consentita a decorrere dal 1 agosto 2019. Con il d. l. 14 giugno 2019, n. 53, convertito in legge 8 agosto 2019, n. 77, in vigore dal 15 giugno 2019, si è ulteriormente posticipata la data di entrata in vigore delle disposizioni artt. 2, 3, 4, 5 e 7 del d.lgs. n. 216/2017. In particolare, il termine "dopo il 31 luglio" è stato posticipato al "dopo il 31 dicembre 2019"; diversamente il termine per l'entrata in vigore del co. 2 d.lgs. 216/2017 (circa la pubblicazione dell'ordinanza cautelare) è posticipato a decorrere dal 1 gennaio 2020.

[5] Cfr. BRONZO, *Intercettazioni ambientali tramite captatore informatico: limiti di ammissibilità, uso in altri processi e divieti probatori*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra, Orlandi, cit., 2018, 235; CASSIBBA, *La circolazione delle intercettazioni tra "archivio riservato" e "captatore informatico"*, *Le nuove intercettazioni,* a cura di Mazza, cit., 101; GIORDANO, *La disciplina del captatore informatico*, in *L'intercettazione di comunicazioni*, a cura di BENE, Bari, 2018, 247 e ss.; SIGNORATO, *Modalità procedimentali dell'intercettazione tramite captatore informatico*, cit., 235.

[6] Con riferimento alle modalità di utilizzo del captatore informativo, v. BRIGHI, *Funzionamento e potenzialità investigative del malware*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra, Orlandi, cit., 221 ss.

Vi sono altre novità legislative, che tuttavia esulano dal contesto qui di interesse ma che incidono sulle valutazioni del giudice, realizzando un possibile ampliamento del controllo giurisdizionale sulle modalità esecutive. Risulta, infatti, modificato anche l'art. 267, co. 1, terzo periodo, nel quale, dopo le parole: "all'articolo 51, co. 3 *bis* e 3 *quater*", sono inserite le seguenti: "e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4". Dunque, il decreto di autorizzazione di intercettazione tra presenti, mediante inserimento di captatore informatico su dispositivo elettronico portatile, deve indicare le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini[6]. Inoltre, il decreto deve indicare i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono qualora si proceda per delitti diversi da quelli di cui all'articolo 51, co. 3 *bis* e 3 *quater*, e per i delitti dei pubblici ufficiali contro la pubblica amministrazione. Nella parte in cui precisa che il giudice delle indagini preliminari deve illustrare le ragioni che portano ad impiegare la modalità informatica per realizzare intercettazioni tra presenti, dunque, la nuova norma sembra estendere l'oggetto della valutazione del Gip anche all'ambito specificamente riservato in precedenza al pubblico

Quanto, invece, alla utilizzabilità del captatore informatico nei procedimenti per i reati contro la pubblica amministrazione, la L. n. 3 del 2019[7] è intervenuta anche in materia di intercettazioni. Nel contesto di discorso, in particolare, l'art. 1, co. 3[8], ha abrogato il secondo co. dell'art. 6 del d. lgs. 216 del 2017, che non consentiva, nei reati contro la pubblica amministrazione, l'utilizzo del captatore informatico nei luoghi di privata dimora, "quando non vi è motivo di ritenere che ivi si stia svolgendo l'attività criminosa". Dunque, con l'abrogazione, l'utilizzo del captatore informatico per i reati contro la pubblica amministrazione è possibile alle medesime condizioni previste per i reati di criminalità organizzata. Il nuovo testo dell'articolo 266, co. 2-*bis*[9], c.p.p., prevede oggi che: "L'intercettazione di comunicazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, co. 3-*bis* e 3-*quater*, e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4". La piena operatività della disposizione è posticipata per effetto dell'ulteriore rinvio operato dal decreto sicurezza *bis*[10], per cui la disciplina si applica alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 dicembre 2019.

2. *Oltre la sentenza Scurato.* Il legislatore ha esteso le norme esistenti alle intercettazioni realizzate tramite captatore informatico, seguendo il percorso

---

ministero. Non vi è dubbio che l'ampiezza del controllo giurisdizionale sia indispensabile per bilanciare l'uso del mezzo informatico in esame nelle investigazioni con la tutela costituzionale del domicilio. Cfr. GIORDANO, *La disciplina del captatore informatico*, cit., 266, secondo cui «L'aspetto che appare più critico riguarda la profondità delle valutazioni che può compiere il Gip. Appare ragionevole ritenere che il decreto del giudice possa finire con il concretizzarsi nella mera riproposizione delle indicazioni contenute nella richiesta del pubblico ministero, che è l'organo che conduce le indagini e che meglio può apprezzare le difficoltà pratiche che possono sussistere". È ben possibile che il decreto del Gip finisca con il contenere mere "formule di stile", prive di un sostanziale contenuto, perché consistenti nell'accoglimento di elementi di fatto che solo il pubblico ministero può apprezzare»

[7] Cfr. CAMON, *Disegno di legge spazzacorrotti e processo penale. Osservazioni a prima lettura*, in *questa Rivista*., 2018, 3, 1 ss.; DE CARO, *La legge c.d. spazza corrotti: si dilata ulteriormente la frattura tra l'attuale politica penale, i principi costituzionali e le regole del giusto processo,* in *Proc. pen. giustizia*, 2019, 2, 281 ss.

[8] Cfr. l. 9 gennaio 2019 n. 3, recante «*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*», in G.U., 16 gennaio 2019, n. 13.

[9] Il co. 4, lett. a), della l. 3 del 2019, prevede che all'articolo 266, co. 2 *bis*, sono aggiunte, in fine, le seguenti parole: «, *e per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, determinata ai sensi dell'articolo 4*».

[10] D. l. 14 giugno 2019, n. 53, convertito in legge 8 agosto 2019, n. 77, in vigore dal 15 giugno 2019.

della sentenza Scurato, ma ha previsto alcuni adeguamenti della disciplina dell'atto tipico per renderlo "compatibile" con la nuova tecnologia[11], tentando di limitare una smodata e possibile acquisizione dei dati.
Vi sono profili apprezzabili della nuova disciplina. Tra questi si ascrive la previsione della inutilizzabilità, desumibile dal raccordo tra gli artt. 267 e 271, co. 1, c.p.p., che risulta rafforzata dalla previsione secondo cui "non sono in ogni caso utilizzabili i dati acquisiti nel corso delle operazioni preliminari all'inserimento del captatore informatico sul dispositivo elettronico portatile e i dati acquisiti al di fuori dei limiti di tempo e di luogo indicati nel decreto autorizzativo" (art. 271, co. 1 *bis*, c.p.p.), così da consentirne la distruzione "salvo che costituisca corpo del reato" (art. 271, co. 3, c.p.p.)[12].
Ugualmente condivisibile[13] è l'intendimento del legislatore di rimediare alle lacune della disciplina dei confini operativi e tecnici. Intendimento tanto meritevole di attenzione perché perseguito, come previsto dalla norma delegante (art. 1, co. 84, lett. a) L. 103 del 2017), lasciando immutati "i limiti e i criteri di utilizzabilità".
I risultati, derivanti dalle modifiche alle disposizioni di attuazione, tuttavia, non sono soddisfacenti e pongono problemi di estrema delicatezza. Al riguardo, sembra difficile sfuggire all'impressione che la soluzione prevista sia il risultato di un compromesso del tutto inadeguato e un po' farisaico: non si è avuto il coraggio di scandagliare i possibili usi distorti del captatore informatico, accettando inconsapevolmente il rischio di una lacuna di tutela della riservatezza, come dimostrano recenti vicende giudiziarie[14].
Il quadro della disciplina è rappresentato dalle modifiche dell'art. 89 disp. att. c.p.p.[15]. Esse coinvolgono diversi interessi. Quando la captazione è compiuta

---

[11] Cfr. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, in *Dir. pen. processo*, 2018, 1210
[12] Cfr. GALANTINI, *L'inutilizzabilità dei risultati*, in *L'intercettazione di comunicazioni*, a cura di BENE, cit., 227 e ss.
[13] Secondo CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, cit., 1210, "appare lodevole la scelta del legislatore di delineare una disciplina tale da consentire l'impiego del *trojan* tenendo contemporaneamente conto delle peculiarità in esso insite, che ne segnano la differenza specifica rispetto alle intercettazioni".
[14] Si pensi allo *spyware*, il cui nome è Exodus, che è stato scoperto dalla società no profit Security Without Borders, in un'inchiesta in collaborazione con la rivista Motherboard. Migliaia di italiani sono stati infettati per errore da un software pensato per intercettazioni di Stato, tramite app inserite su Google Play Store. Il sistema Exodus, utilizzato dalle procure, quale programma spia per le intercettazioni, ha consentito una intercettazione indiscriminata.
[15] Sull'utilizzo dei captatori in generale, la riforma di cui al d.lgs. 216 del 2017, in attuazione della delega di cui alla l. 103/2017, ha previsto modifiche dell'art. 89 disp. att c.p.p. In attesa della piena operatività delle disposizioni generali sull'uso del captatore, l'esecuzione di tali forme di captazioni in tema crimina-

mediante un programma informatico del tipo *trojan* introdotto in un dispositivo elettronico portatile, il verbale deve indicare "il tipo di programma impiegato" ed "i luoghi in cui si svolgono le comunicazioni o le conversazioni" (art. 89 disp. att. co. 1). L'intento è quello di creare la condizione per una effettiva verifica dello strumento usato da parte della difesa.

In attuazione di una specifica previsione della legge delega, all'art. 1, co. 84, lett. e), n. 5, è stabilito che, per le intercettazioni tramite captatore informatico, devono essere utilizzati soltanto programmi conformi a requisiti tecnici fissati con un decreto ministeriale da emanare entro trenta giorni dalla data di entrata in vigore dei decreti legislativi di riforma del codice di rito. Il co. 2-*bis* dell'art. 89 disp. att., sul punto, prevede che: "ai fini dell'installazione e dell'intercettazione attraverso captatore informatico in dispositivi elettronici portatili possono essere impiegati soltanto programmi informatici conformi ai requisiti tecnici stabiliti con decreto del Ministro della giustizia"[16]. La previsione ha trovato attuazione deludente. Il decreto ministeriale avrebbe dovuto tener costantemente conto dell'evoluzione tecnica al fine di garantire che tali programmi si limitassero ad effettuare le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, di sicurezza e di efficacia. L'idea sottesa sembra diretta a scongiurare il rischio di utilizzare software più evoluti, capaci di compiere attività più penetranti, come, per esempio, la perquisizione a distanza del dispositivo bersaglio. Ma le aspettative, allo stato, sono disattese: il decreto ministeriale di riferimento è il D.M. 20 aprile 2018[17], il cui art. 4 prevede i requisiti tecnici dei programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore. È interessante notare che il provvedimento non tiene conto del parere del Garante della privacy[18]

---

lità organizzata, terrorismo e p.a. dovranno essere valutate e eseguite in conformità alle indicazioni del testo originario degli artt. 266 e 267 c.p.p. sulla base delle indicazioni fornite dalle Sezioni unite Scurato.

[16] È stato da tempo suggerita la necessità di garantire che il programma informatico di captazione non alteri i dati acquisiti, né le restanti funzioni del dispositivo, v. ATERNO, *Mezzi atipici di ricerca della prova e nuovi strumenti investigativi informatici: l'acquisizione occulta da remoto e la soluzione per la lotta contro l'utilizzo del cloud criminal*, in *IISFA Memberbook 2012 Digital Forensics. Condivisione della conoscenza tra i membri dell'IISFA Italian Chapter*, a cura di Costabile, Attanasio, Forlì 2013, 1 e ss.

[17] In tema di disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, co. 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216

[18] V. Parere del Garante della *privacy* sullo schema di decreto del Ministro della giustizia recante disposizioni di attuazione per le intercettazioni mediante inserimento di captatore informatico e per l'accesso all'archivio informatico a norma dell'articolo 7, co. 1 e 3, del decreto legislativo 29 dicembre 2017, n. 216, (12 aprile 2018).

che individuava, ad esempio, la necessità di integrare la norma di riferimento, specificando le misure tecniche da adottare al fine di garantire la riservatezza dei dati sui sistemi funzionali all'esecuzione delle intercettazioni mediante captatore informatico[19].

Ancora. Il co. 2-*ter* dell'art. 89 disp. att. c.p.p. prevede che nei casi indicati dal co. 2-*bis* "le comunicazioni intercettate sono trasferite, dopo l'acquisizione delle necessarie informazioni in merito alle condizioni tecniche di sicurezza e di affidabilità della rete di trasmissione, esclusivamente verso gli impianti della procura della Repubblica". La disposizione ha una *ratio* chiara: vuole impedire la cd. remotizzazione della registrazione che è molto diffusa nella prassi, tant'è che secondo un discutibile indirizzo giurisprudenziale consolidato, essa non incide sulla genuinità del dato registrato[20]. E, dunque, attuando la direttiva contenuta nell'art. 1, co. 84, lett. e), n. 4, della L. n. 103 del 2017, la previsione limita la possibilità della trasmissione dei dati al loro invio solo al server della procura. Il legislatore, quindi, sembra aver ben chiaro il pericolo che il trasferimento dei dati possa determinarne la diffusione, al punto da prevedere che, durante il trasferimento dei dati, siano "operati controlli costanti di integrità, in modo da assicurare l'integrale corrispondenza tra quanto intercettato e quanto trasmesso e registrato".

---

[19] Così il Garante della *privacy*, cfr. Parere, cit., 12 aprile 2018, in riferimento all'articolo 4 dello schema che definisce i requisiti tecnici dei c.d. "programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore", a norma dell'art. 7, co. 1, del decreto legislativo 29 dicembre 2017, n. 216. Al fine di chiarire cosa si intenda per "programmi informatici funzionali all'esecuzione delle intercettazioni mediante captatore", è necessario specificare se in tale categoria siano ricompresi uno o più dei seguenti moduli software che, comunemente, compongono un sistema di intercettazione mediante captatore informatico (es. il software che, installato sui dispositivi target, opera l'acquisizione delle informazioni; il sistema di inoculazione; il sistema di gestione; ecc.). Si rileva, inoltre, la necessità di integrare il suddetto articolo indicando in modo puntuale le misure tecniche da adottare al fine di garantire la riservatezza dei dati sui sistemi funzionali all'esecuzione delle intercettazioni mediante captatore informatico, specificando ad esempio: a) le modalità di accesso ai citati sistemi da parte degli operatori autorizzati; b) le funzionalità di registrazione delle operazioni svolte sui citati sistemi dagli operatori; c) le modalità di trasmissione dei dati acquisiti mediante captatore. Infine, è necessario prevedere nello schema che l'installazione del captatore informatico su un dispositivo elettronico portatile non deve, ove possibile, abbassare il livello di sicurezza del medesimo dispositivo in cui è stato installato, sia nel corso delle operazioni di intercettazione, che al termine delle stesse. Ciò al fine di impedire che il dispositivo possa essere compromesso da terzi, con eventuali riflessi negativi sulla protezione dei dati personali ivi contenuti nonché sull'attività investigativa".

[20] Sulla legittimità della prassi della cd. remotizzazione, si veda Cass., Sez. un., 26 giugno 2008, n. 36359, in *Mass. Uff.,* n. 240395. L'orientamento è costante; di recente Cass., sez. VI, 17 novembre 2015, n. 47504, in *Cass. pen.*, 2016, 6, 2572; Cass., sez. I, 21 ottobre 2015, n. 49918, inedita; Cass., sez. IV, 27 novembre 2014, n. 5401, in *Mass. Uff.*, n. 262126; Cass., sez. VI, 4 novembre 2014, n. 53418, in *Mass. uff.*, n. 261838; Cass., sez. III, 7 gennaio 2014, n. 1116, in *Mass. Uff.*, n. 259744.

Il successivo co. 2-*quater* dell'art. 89 disp. att. c.p.p. sottende che l'intercettazione tramite captatore presuppone l'immediata trasmissione dei dialoghi carpiti. La norma, attenta alle prassi, prende atto che talvolta il contestuale trasferimento dei dati intercettati non è praticabile. L'impossibilità può dipendere da diverse ragioni tecniche, tra queste, ad esempio, la mancanza di connessione internet. In via generale, bisogna anche impedire che la trasmissione dei dati possa essere a sua volta intercettata e, di conseguenza, che le intercettazioni in atto possano essere svelate. In questo caso, dunque, "il verbale di cui all'articolo 268 del codice dà atto delle ragioni tecniche impeditive e della successione degli accadimenti e delle conversazioni intercettate".
Vera norma di garanzia è prevista nel nuovo art. 89, co. 2-*quinquies*, disp. att. c.p.p. secondo cui: "al termine delle operazioni si provvede, anche mediante persone idonee di cui all'articolo 348 del codice, alla disattivazione del captatore con modalità tali da renderlo inidoneo a successivi impieghi". Anche in questo caso, la disposizione dà attuazione ad una direttiva dettagliata della legge delega n. 103 del 2017, contenuta nell'art. 1, co. 4, lett. e), n. 4. Si vuole evitare che il dispositivo possa essere silente ed azionato a distanza di tempo, magari al di fuori di una autorizzazione giudiziaria[21].
La costruzione dei confini operativi del captatore informatico è determinata da propositi condivisibili ma i risultati sono destinati ad essere inefficaci. Un buon governo di questo comparto avrebbe dovuto tener conto del cambiamento sostanziale del sistema intercettativo: se si ritenesse che oggi alcuni interessi rilevanti corrono un rischio insopportabile, sarebbe doveroso un intervento coordinato di riassetto normativo per una efficace tutela e, invece, sorprendentemente, il quadro normativo esistente non prevede regole confortate da sanzioni. L'indirizzo giurisprudenziale consolidato, infatti, riteneva che l'inosservanza delle disposizioni previste dall'art. 89 disp. att. c.p.p., in tema di verbali e nastri registrati delle intercettazioni, non determinasse l'inutilizzabilità degli esiti dell'attività captativa legittimamente disposta ed eseguita[22]. L'orientamento appare ancora attuale, non essendo stato aggiornato l'art. 271, co. 1, c.p.p.[23]. Nessun rilievo assumono, dunque, gli effetti della

[21] Cfr. CONTI, *Prova informatica e diritti fondamentali: a proposito di captatore e non solo*, cit., 1210; GIORDANO, *La disciplina del captatore informatico*, cit., 278.
[22] Cass., Sez. I, 2 dicembre 2009, n. 8836, in *Mass. uff.,* n. 246377; Cass., Sez. IV, 17 settembre 2004, n. 49306, in *Mass. uff.*, n. 229922; Cass., sez. IV, 14 gennaio 2004, n. 17574, in *Mass. Uff.*, n. 228173; Cass., Sez. VI, 26 ottobre 1993, n. 11421, in *Mass. uff.*, n. 198560; di recente, anche Cass., Sez. V, 19 gennaio 2018, n.15472; Cass., Sez. III, 17 febbraio 2015, n. 20418, in *Cass. pen.*, 2016, 1, 313.
[23] Cfr. GALANTINI, *Profili di inutilizzabilità delle intercettazioni anche alla luce della nuova disciplina*, cit., 12.

eventuale violazione delle regole concernenti il ricorso al captatore informatico per il quale sono previste specifiche prescrizioni, che appunto vanno dalla indicazione nel verbale del tipo di programma impiegato (art. 89 co.1), al ricorso a programmi conformi a requisiti tecnici indicati dal Ministero (art. 89 co. 2-*bis*), al trasferimento delle comunicazioni esclusivamente verso gli impianti della procura (art. 89 co.2-*ter*), alla disattivazione del captatore con modalità tali da renderlo inidoneo a successivi impieghi (art. 89 co. 2-*quinquies*).

3. *La effettiva direzione delle indagini: i rapporti tra polizia giudiziaria ed ausiliari.* Al legislatore non è sfuggita la potenzialità dello strumento tecnologico, con l'art. 4, co. 1, lett. c), del d. lgs. n. 216 del 2017, ha aggiunto all'art. 268, co. 3-*bis*, c.p.p. un nuovo periodo, in forza del quale "per le operazioni di avvio e di cessazione delle registrazioni, mediante inserimento di captatore informatico su dispositivo elettronico portatile, riguardanti comunicazioni e conversazioni tra presenti, l'ufficiale di polizia giudiziaria può avvalersi di persone idonee di cui all'articolo 348, co. 4". In questi termini, assume rilievo il delicato rapporto che intercorre con le società incaricate per il servizio di intercettazione a mezzo captatore *ex* art. 348, co. 4, c.p.p.
Il rischio concreto è legato alla ineffettività dell'attuale disciplina che regola il contributo alle indagini degli ausiliari di polizia giudiziaria. Secondo l'art. 348, co. 4, c.p.p., infatti, quando, di propria iniziativa o a seguito di delega del pubblico ministero, la polizia giudiziaria compie atti od operazioni che richiedono specifiche competenze tecniche, essa può ricorrere a persone idonee.
Ineffettività della disciplina che, dunque, deriva dalla inadeguatezza della previsione normativa rispetto alla peculiarità ed alla oscillazione dimensionale del mezzo investigativo, laddove, il pericolo riguarda la compromissione e l'alterabilità dei dati giudiziari, poiché non sono regolate le particolari modalità di realizzazione delle captazioni, da parte delle società incaricate *ex* art. 348, co. 4, c.p.p. In particolare, vi è totale assenza di una disciplina delle modalità di acquisizione delle tecnologie rivolte e destinate alla captazione di comunicazioni e, più in generale, si riscontra la mancanza di linee guida ministeriali, dirette a regolamentare i rapporti con le società di intercettazione[24]. Come risulta da alcune vicende giudiziarie, ad esempio, si è realizzata la delocalizzazione dei server in territori non soggetti alla giurisdizione nazionale. La

[24] Sulla necessità di una guida da parte del Ministero della giustizia vi è unanime richiesta dei procuratori.

vicenda giudiziaria è ancora in corso. Essa coinvolge una società "sviluppatrice di piattaforme informatiche e di software per lo svolgimento di intercettazioni telematiche mediante captatore informatico". Tra le piattaforme anche *Exodus*, utilizzata, per le intercettazioni tramite *trojan*, da aziende, divenute ausiliari della polizia giudiziaria. L'indagine dovrà accertare le caratteristiche di funzionamento della piattaforma informatica e le modalità con cui i dispositivi degli utenti venivano infettati, dopo aver scaricato una particolare app. Il sospetto è che sia stato effettuato un numero infinito di intercettazioni non autorizzate dall'autorità giudiziaria, tramite un virus utilizzato dalle società, i cui dati sarebbero stati conservati in spazi cloud della piattaforma Amazon, con sede negli Stati Uniti. La gravità dell'operazione sembra non arrestarsi, almeno fino a quando non verranno individuati i limiti del contratto di sperimentazione che i servizi segreti italiani avevano stipulato nel 2016 con la stessa società che gestiva *Exodus*.

Il rischio concreto, strettamente connesso alla partecipazione di soggetti estranei alla polizia giudiziaria, come è evidente, è legato proprio all'assenza di un vuoto di tutela dei diritti degli interessati e della stessa segretezza delle indagini[25]. In prospettiva, è utile ricordare che il Garante della *privacy* ha già suggerito di: a) ricorrere all'integrazione del decreto ministeriale del 20 aprile 2018; b) novellare il decreto legislativo n. 216 del 2017[26]. Tali sollecitazioni hanno trovato parziale recepimento in una comunicazione del Ministro della Giustizia al Garante in data 18 luglio 2019, con cui sono state indicate solo alcune linee di riforma che il Guardasigilli intende seguire per limitare i rischi di un uso deviato dei software-spia: in particolare, si propone l'adozione di misure volte ad indirizzare le conversazioni intercettate esclusivamente verso gli impianti della procura, con adeguati controlli sull'integrità dei contenuti e sui requisiti tecnici dei captatori, tali da garantire che essi si limitino effettivamente ad eseguire le sole operazioni autorizzate.

In via generale, stupisce che ancora non siano prese in considerazione le progressive evoluzioni dello strumento intercettativo[27]. Il tema dei controlli, non

---

[25] Si veda BRIZZI, *Il captatore informatico: un Exodus verso " buone pratiche"?*, in *www.ilpenalista.it,* secondo cui *" Il ricorso a tali due tipologie di sistemi (app o comunque software che non siano inoculati direttamente sul dispositivo-ospite, ma scaricati da piattaforme liberamente accessibili a tutti e, per altro verso, archiviazione mediante sistemi* cloud in server *posti fuori dal territorio nazionale) dovrebbe, dunque, essere oggetto di un apposito divieto*".

[26] La cui efficacia, relativamente al profilo in esame, era originariamente differita ai provvedimenti autorizzativi emessi dopo il 31 luglio prossimo, termine poi prorogato dal cd. decreto sicurezza *bis*, decreto-legge, 14 giugno 2019 n. 53, convertito dalla l. 8 agosto 2019, n. 77, al 31 dicembre 2019.

[27] Conferma è offerta nel parere del garante della Privacy, cit. Pur apprezzando tale indirizzo, il Garante lo ritiene ancora insufficiente a "ricomprendere le varie e più complesse implicazioni che uno strumen-

particolarmente definiti, sui soggetti ausiliari apre a rapporti opachi nell'attività di indagine e mette in discussione l'effettiva direzione delle indagini preliminari, che è funzione propria del pubblico ministero ed impone il rispetto della legalità del procedimento.
L'esame della giurisprudenza prevalente corrobora le perplessità, laddove assicura alla polizia giudiziaria ampia discrezionalità quanto alla scelta dell'ausiliario. Ai fini dell'utilizzabilità in fase di indagine preliminare dei risultati degli accertamenti tecnici compiuti dalla polizia giudiziaria con il ricorso ad attività collaborativa, si rileva, dunque, che non occorre che gli ausiliari siano individuati con l'osservanza delle forme e delle modalità previste per la nomina del consulente tecnico del pubblico ministero. Né sono previste particolari incompatibilità. Prova ne è l'orientamento secondo cui, ad esempio, può essere nominato ausiliario di polizia giudiziaria per lo svolgimento di attività tecniche il soggetto che sia stato già sentito come persona informata sui fatti[28]. Dunque, non sono previste particolari forme per il conferimento dell'incarico di ausiliario[29], né è richiesto l'impiego di una forma scritta[30].
La storia dei rapporti tra polizia giudiziaria ed ausiliari non è recente, come dimostra l'esame delle prassi seguite tutte le volte in cui si usano mezzi tecnologici per compiere indagini e la polizia giudiziaria deve ricorrere ai soggetti che hanno le competenze tecniche richieste. Si è detto, ad esempio, in un caso in cui l'attività di messa in chiaro di messaggi criptati erano scambiati mediante il sistema Blackberry, che la decifrazione "è avvenuta con l'intervento di ausiliari tecnici nominati dalla polizia giudiziaria, la cui nomina è consentita senza particolari formalità"[31]. E quanto alla spontanea collaborazione in ordine all'algoritmo (chiave di decifrazione) per effettuare la traduzione in chiaro offerta dal produttore Blackberry, da parte di RIM Italia, si è ribadito che la stessa afferisce a comportamenti di quotidiana cooperazione con l'autorità giudiziaria[32]. Seguendo questa linea di ragionamento, l'indirizzo giurisprudenziale ha ritenuto legittima l'attività di messa in chiaro di messaggi criptati, scambiati mediante il sistema Blackberry, anche se effettuata dalla polizia giudiziaria attraverso la nomina, pure senza particolari formalità, di ausiliari

---

to tanto prezioso quanto invasivo – quale quello delle intercettazioni – ha sul sistema delle libertà individuali".
[28] Cass., Sez. V, 24 marzo 2017, n. 23021, in *Mass. Uff.*, n. 270376.
[29] Cass., Sez. III, 18 febbraio 2010, n. 17177, in *Mass. Uff.*, n. 246978.
[30] Cass., Sez. III, 27 gennaio 1998, n. 3840, in *Mass. Uff.*, n. 210329.
[31] Cass., Sez. III, 5 marzo 2009, n. 16683, in *Mass. Uff.*, n. 243462
[32] Cass., Sez. III, 10 novembre 2015, n. 5818, in *Mass. Uff.* n. 266267, volendo, BENE, *Transnazionalità dei crimini nella società confessionale,* in *Giur. it.,* 2016, 3, 717 e ss.

tecnici, ed il ricorso alla spontanea collaborazione da parte del produttore del sistema operativo, che ha concesso l'uso dell'algoritmo necessario per la decifrazione[33]. Peraltro, seguendo un orientamento consolidato[34], ancor di più si afferma che l'impiego di ausiliari tecnici, come gestori dei sistemi informatici utilizzati, "è assolutamente necessario per realizzare l'attività investigativa". E' stata così esclusa la necessità di rogatoria internazionale quando le comunicazioni sono avvenute in Italia pure nei casi in cui per "decriptare" i dati identificativi associati ai codici PIN sia stato necessario ricorrere alla collaborazione del produttore del sistema operativo avente sede all'estero[35].
In prospettiva, il pericolo della "fragilizzazione" dei diritti fondamentali appare sempre più concreto. Il d.lgs. 18 maggio 2018, n. 51[36] fissa gli obblighi del titolare del trattamento dei dati e, allo stesso modo[37], delinea i doveri del responsabile del trattamento[38], ma, come è noto, non individua anche i "titolari del trattamento dei dati" in ambito giudiziario[39]. La previsione è, invece, contenuta nell'art. 2-*sexiesdecies* codice *privacy* (Responsabile della protezione dei dati per i trattamenti effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni) inserito dall'art. 2, co. 1, lett. f), d.lgs. 10 agosto 2018, n. 101 e in vigore dal 19 settembre 2018: il responsabile della protezione dati è designato, a norma delle disposizioni di cui alla sezione 4 del capo IV del Rego-

[33] Cass., Sez. III, 10 novembre 2015, n. 5818, cit.
[34] Cass., Sez. III, 10 novembre 2015, n. 50452, in *Cass. pen.,* 2016, 7-8, 2941; Cass., Sez. III, 5 marzo 2009, n. 16683, inedita. Di recente Cass., Sez. VI, 27 novembre 2018, n. 14395, per un commento v. GIORDANO, *Blackberry Messenger: l'indisponibilità dell'algoritmo per decriptare i dati informatici non lede il diritto di difesa,* in *www.ilpenalista.it*
[35] Cass., Sez. IV, 8 aprile 2016, n. 16670, in *Mass. uff.,* n. 266983.
[36] In attuazione della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio.
[37] L'art. 15 stabilisce che: 1. Il titolare del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi per i diritti e le libertà delle persone fisiche, mette in atto misure tecniche e organizzative adeguate per garantire che il trattamento sia effettuato in conformità alle norme del presente decreto. 2. Le misure di cui al co. 1 sono riesaminate e aggiornate qualora necessario e, ove proporzionato rispetto all'attività di trattamento, includono l'attuazione di politiche adeguate in materia di protezione dei dati da parte del titolare del trattamento.
[38] Cfr. art. 18, d.lgs. 18 maggio 2018, n. 51
[39] Viceversa, l'art. 46 del Codice della privacy, abrogato dal d.lgs. 10 agosto 2018, n. 101 (di adeguamento del Codice privacy al regolamento UE 2016/679), prevedeva che «gli uffici giudiziari di ogni ordine e grado, il Consiglio superiore della magistratura, gli altri organi di autogoverno e il Ministero della giustizia sono titolari dei trattamenti di dati personali relativi alle rispettive attribuzioni conferite per legge o regolamento».

lamento, anche in relazione ai trattamenti di dati personali effettuati dalle autorità giudiziarie nell'esercizio delle loro funzioni[40]. Con riferimento alla vicenda *Exodus*[41], il dubbio, dunque, riguarda una possibile e ulteriore situazione di anomia disapplicativa, imputabile sì alla complessità del sistema di protezione delle persone fisiche, con riguardo al trattamento dei dati personali, ma che si riflette direttamente sulla nomina del responsabile del procedimento.

[40] Quindi la nomina del DPO, in Italia, sfugge alla regola di esenzione europea che dispensa le autorità giurisdizionali dalla nomina di questa figura nell'esercizio di tali funzioni. V. BRIZZI, *Il captatore informatico: un Exodus verso "buone pratiche"?,* cit.

[41] Cfr. Cass., Sez. VI, 26 aprile 2019, n. 31579, per un commento cfr. BRIZZI, *Il captatore informatico: un Exodus verso "buone pratiche"?,* cit.