

QUESITI

ROBERTO RAMPIONI

Captatore informatico e delitti dei pubblici ufficiali contro la P.A. Le Sezioni unite civili riconoscono, in modo erroneo, la immediata applicabilità della legge cd. “Spazzacorrotti”.

Le Sezioni unite civili riconoscono -in modo erroneo- la immediata applicabilità della legge cd “Spazzacorrotti” alla disciplina del “captatore informatico” dettata dal d.lgs. n. 216 del 2017 per i delitti dei pubblici ufficiali contro la pubblica Amministrazione.

Computer collector and crimes of public officials against the P.A. The joined sections civilians recognize, erroneously, the immediate applicability of the “Spazzacorrotti” law

The Civil Plenary Section of the Supreme Court recognize -wrongly- the prompt enforceability of “Spazzacorrotti” law at the discipline of the “computer programmer” ruled by d.lgs. n. 216/2017 in order to investigate public officials crimes against public administration.

SOMMARIO: 1. Potenzialità intrusiva del trojan horse e diritto alla “libertà informatica”. - 2. L’impiego del captatore informatico nei processi di criminalità organizzata. - 3. La disciplina del captatore informatico introdotta dal decreto legislativo n. 216 del 2017. - 4. L’estensione dell’operatività del captatore informatico ai delitti dei pubblici ufficiali contro la P.A. La posizione della dottrina circa la (non) immediata applicabilità della legge cd. “Spazzacorrotti”. - 5. Il diverso orientamento delle Sezioni unite civili. - 6. Osservazioni critiche.

1. Potenzialità intrusiva del trojan horse e diritto alla “libertà informatica”. A dispetto della potenzialità intrusiva dei “captatori informatici” l’intervento legislativo in materia (d. lgs. n. 216 del 2017) si è concentrato - sulla scia, in particolare, della pronuncia delle Sezioni unite del 28 aprile 2016 (n. 26889, Scurato) - su una sola delle possibili finalità investigative; quella che mira ad intercettare comunicazioni fra presenti.

La legge di riforma in materia si è, dunque, imposta - analogamente alla giurisprudenza - una sorta di *self restraint* limitandosi a “disciplinare le intercettazioni di comunicazioni fra presenti mediante immissione di captatori informatici”, come testualmente recita la direttiva delegante contenuta nell’art. 1, co. 84, lett. e) legge 23 giugno 2017 n. 103.

Un simile strumento tecnologico consente, tuttavia, numerose e diverse attività¹:

¹ In argomento v., in generale, TURCO, *La ricerca della prova ad alta efficacia intrusiva: il captatore elettronico*, in *La riforma della giustizia penale, Commento alla legge 23 giugno 2017 n. 103*, a cura di A. Scalfati, Torino, 2017, 307 s.

- captare il traffico dati in arrivo o in partenza dal dispositivo “infettato” (navigazione e posta elettronica, sia *web mail* che *out look*);
- 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;
- mettere in funzione la *web camera*, permettendo di carpire immagini;
 - perquisire lo *hard disk* e di fare copia, totale o parziale, delle unità di memoria del sistema informatico preso di mira;
 - decifrare tutto ciò che viene digitato sulla tastiera collegata al sistema (*keylogger*) e visualizzare ciò che appare sullo schermo del dispositivo bersaglio (*screenshot*);
 - sfuggire agli antivirus in commercio.

È, pertanto, con fondamento che si è inteso rilevare che “il lato discutibile della scelta legislativa sta nell’aver dato per scontato che il solo diritto fondamentale da tutelare di fronte all’uso investigativo dei captatori informatici sia la libertà e segretezza della comunicazione in ambito domiciliare. Non è così. Le tecnologie informatiche oggi disponibili consentono di acquisire informazioni che vanno ben oltre lo spazio protetto dall’art. 15 Cost., quello della comunicazione interpersonale...tramite esse è possibile osservare e controllare l’insieme delle relazioni sociali della persona presa di mira, le sue frequentazioni sul *web*, i frammenti della sua esperienza ricavabili da documenti scritti, fotografici, audio, video”².

Questa formidabile potenzialità investigativa del “captatore informatico” (cd. *trojan horse* o agente intrusore) – si soggiunge – ha portato la Corte costituzionale tedesca – già nel 2008 e, poi, ancora nel 2016 – ad affermare l’esistenza di un diritto fondamentale: il *diritto all’uso confidenziale dei sistemi informatici* (altrimenti detto, *diritto fondamentale alla intimità digitale* ov-

² Così ORLANDI, *Usi investigativi dei cd. captatori informatici. Criticità e inadeguatezza di una recente riforma*, in *Riv. it. dir. proc. pen.*, 2018, 540. Osserva in senso critico GIOSTRA, *I nuovi equilibri tra diritto alla riservatezza e diritto di cronaca nella riformata disciplina delle intercettazioni*, in *Riv. it. dir. proc. pen.*, 2018, 522: “Le intercettazioni di comunicazioni e di conversazioni costituiscono lo strumento investigativo che geneticamente incuba i più gravi rischi per la *privacy* dei cittadini. Rischi che diventano esponenzialmente maggiori qualora le intercettazioni siano effettuate con il captatore informatico, che ha un allarmante potenziale invasivo della sfera privata, a cui corrisponde una straordinaria efficacia esplorativa e acquisitiva. Efficacia troppo preziosa perché l’inquirente resista alla tentazione di avvalersene in modo indiscriminato, se non vincolato da una rigorosa demarcazione legislativa dei suoi confini operativi. Meritoriamente, pertanto, la recente riforma (d.lgs. n. 216 del 2017) ha focalizzato l’attenzione su queste due gravi carenze della normativa in materia: l’inaccettabile disinteresse per la riservatezza dei soggetti coinvolti nelle conversazioni captate e l’assenza di qualsiasi regolamentazione normativa dell’uso investigativo dell’insidiosa risorsa tecnologica rappresentata dai *trojan horses*”.

vero al *domicilio informatico*)³. E tale diritto viene evinto dall'obbligo che incombe sullo Stato di proteggere la "dignità" delle persone e il "libero sviluppo della loro individualità" (artt. 1 e 2 *Grundgesetz*) rispetto a qualsiasi aggressione esterna, non esclusa quella proveniente dall'autorità pubblica. Lo schema argomentativo è chiaro: ove emerga la possibilità di una compressione del libero sviluppo della personalità, lì occorrerà riconoscere l'esistenza di un diritto individuale che lo Stato deve garantire.

I rilievi e le affermazioni del *Bundesverfassungsgericht* in tema di "libertà informatiche" valgono, in linea generale, anche per l'ordinamento italiano nel limite in cui si legga, correttamente, l'art. 2 Cost.: norma che fa riferimento a un "elenco aperto" di diritti inviolabili, da aggiornare in ragione delle sfide provocate dal progresso tecnologico e dal correlato evolversi delle sensibilità giuridico-culturali.

Com'è notorio, definire inviolabile un diritto non impedisce che lo si possa limitare per il compimento di attività – quali quelle riguardanti la prevenzione e repressione dei reati – reputate fondamentali per la "sicurezza-stabilità sociale". Tema centrale di un dibattito, già ampio, è il rapporto tra sicurezza collettiva e diritto alla riservatezza individuale: esigenze sociali di giustizia, tutela dei diritti personali e necessario bilanciamento in linea con i criteri di ragionevolezza e proporzionalità (come indicati, peraltro, dalla Corte EDU)⁴. Le forti criticità emerse in argomento scaturiscono dalla difficoltà di "bilanciare esigenze divergenti e tendenzialmente antinomiche"⁵. Comunque sia, la inclusione del diritto in discorso nell'area dei diritti fondamentali – osserva Orlandi – detta, sempre e comunque, particolari cautele nel regolamentarne la compressione: *riserva di legge dei casi e dei modi della limitazione del diritto medesimo nonché motivata autorizzazione giudiziale nel rispetto del principio di proporzionalità*.

³Bundesverfassungsgericht, 27 febbraio 2008, www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html
 Bundesverfassungsgericht, 21 giugno 2016, https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2016/06/rs20160621_2bvr272813en.html;sessionid=30000D90B852DDDF839147628A91C6D.1_cid393. (entrambe anche in versione inglese).

⁴ Corte EDU, 29 marzo 2005, *Matheron c. Francia*,

⁵ BENE, "Il re è nudo": anomalie disapplicative a proposito del captatore informatico, in *questa Rivista*, 2019, n. 3, 1 s., il quale rileva: "L'intento è di rilevare un profilo di crisi del sistema operativo del captatore informatico 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".

Dunque, riconoscere l'esistenza di un "nuovo" diritto fondamentale -*la libertà informatica*- impone necessariamente di ricondurre l'uso investigativo dei captatori informatici alla nota procedura che le Costituzioni moderne, appunto, esigono per la limitazione dei diritti considerati inviolabili: vale a dire, riserva di legge e autorizzazione giudiziale nel rispetto del principio di proporzionalità. La mancata osservanza di queste garanzie (non solo) procedurali va, pertanto, apprezzata quale violazione di un divieto (implicito) di acquisizione del dato probatorio. Il rischio, ragionando diversamente, è quello di lasciare alla polizia giudiziaria - attraverso l'uso di strumenti invasivi della sfera intima della persona - ampi spazi di iniziativa informale e atipica.

È per ciò che le cd. perquisizioni *on-line* sono da considerarsi illegittime fino a che non saranno regolate da una norma volta ad attuare le accennate garanzie procedurali imposte dalla Costituzione per la limitazione di diritti inviolabili. Ed il discorso corre analogamente per l'uso di captatori informatici quali mezzi di intercettazione <<alternativi>> a quelli già regolati dalla legge processuale⁶.

2. *L'impiego del captatore informatico nei processi di criminalità organizzata.* Fino alla riforma del 2017 il mezzo di ricerca della prova in esame non era normativamente previsto e la giurisprudenza inquadrava l'impiego del "*trojan horse*" nell'art. 266, co. 2, c.p.p. come mezzo di "intercettazione ambientale", la cui "natura itinerante" induceva ad escludere <<la possibilità di compiere intercettazioni nei luoghi indicati dall'art. 614 c.p. [...] non potendosi prevedere, all'atto dell'autorizzazione, i luoghi di privata dimora nei quali il dispositivo elettronico verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto del presupposto, previsto dall'art. 266, co. 2, c.p.p. che in detto luogo si stia svolgendo l'attività criminosa>> (in tal senso, da ultimo, Sez. un., 28 aprile 2016, n. 26889, *cit.*).

Tale <<regola>> subiva la sola eccezione - prevista dall'art. 13 d.l. n. 152 del 1991 (poi integrato dall'art. 13 del d.l. 8 giugno 1992 n. 306) - delle indagini per i <<delitti di criminalità organizzata>> (oltre che per il delitto di <<minaccia col mezzo del telefono>>), in relazione ai quali si era inteso statuire che, in presenza di indizi *sufficienti* (e, quindi, non gravi, come oggi prescritto dall'art. 267 c.p.p.), si potesse procedere alle *necessarie* (e, quindi, non assolutamente indispensabili) intercettazioni di scambi comunicativi intrattenuti tra presenti, anche nei luoghi di cui all'art. 614 c.p. e pur in assenza di una

⁶ Così ORLANDI, *op. cit.*, 543.

attività criminosa ivi in corso⁷.

Il d.lgs. n. 216 del 2017 nel codificare per la prima volta l'utilizzabilità del captatore informatico per l'intercettazione tra presenti (art. 266, co. 2, primo periodo), ha mantenuto ferma la regola (sancita per tutte le forme di intercettazione ambientale) per cui la captazione nei luoghi di cui all'art. 614 c.p. è consentita soltanto se vi è fondato motivo di ritenere che ivi sia in corso l'attività criminosa, ampliando tuttavia la disciplina derogatoria ad essa regola. Da un lato, infatti, ha reso <<sempre possibile>> l'intercettazione ambientale nei <<procedimenti per i delitti di cui all'articolo 51, co. 3 *bis* e 3 *quater*>> c.p.p. (art. 266, co. 2 *bis*); dall'altro, ha esteso il regime delle intercettazioni cd. <<antimafia>>, previste dal citato art. 13 d. l. n. 152 del 1991, ai delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni (art. 6, co. 1), *vietando però di effettuarle, solo in questo caso, nei luoghi di privata dimora ed assimilati in assenza di motivi per ritenere in corso di svolgimento l'attività criminosa* (art. 6, co. 2).

3. *La disciplina del captatore informatico introdotta dal decreto legislativo n. 216 del 2017. L'intercettazione <<ambientale>> “può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile”.* Emerge subito chiara - osserva Orlandi, illustrando la disposizione - la duplice limitazione contenuta nel testo dell'art. 266, 2° co., cpp, come novellato dal d. lgs. n. 216 del 2017: il captatore può essere usato solo quale mezzo di *intercettazione ambientale* ed impiegato soltanto su *dispositivi portatili*. Non sono previsti (e, pertanto, non sono ammessi) usi diversi da quello appena ricordato, come ad esempio, perquisizioni *on line* o intercettazioni di messaggi in uscita con il controllo a distanza del *software* di comunicazione (es. programmi *e-mail*, *Messenger*, *WhatsApp*); né possono essere controllati i *computers* fissi. Il discorso, quindi, è circoscritto ai *computers* portatili, ai *tablet*, agli *smartphone*.

L'ampiezza nell'uso del mezzo investigativo è diversificata in ragione della gravità del reato da accertare.

⁷ La norma per questo tipo di reati ha inoltre ampliato i termini di durata massima di intercettazione (quaranta giorni, in luogo di quindici) nonché delle possibili proroghe (venti giorni, in luogo di quindici). Il contenuto dell'art. 13 è stato integrato dal disposto del d.l. 8 giugno 1992 n. 306 (convertito con modificazioni nella legge 7 agosto 1992) per il quale “quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo ad un delitto di criminalità organizzata e che avvenga nei luoghi indicati all'art. 614 c.p., l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa”.

In relazione alla generalità dei delitti che ammettono le intercettazioni (art. 266, 1° co.), il captatore può essere usato per acquisire conversazioni sia *extra*, sia *infra* domiciliari, ma queste ultime, in linea generale, sono legittime solo se vi è motivo di ritenere che nel domicilio sia in corso l'attività criminosa <<oggetto di accertamento>>⁸.

L'intercettazione è, tuttavia, sempre consentita pure nei luoghi di privata dimora, nei procedimenti di cui all'art. 51 co. 3-*bis* e 3-*quater* e, cioè, quando si tratta di accertare reati riconducibili alla nozione (altrimenti vaga e indefinita) di criminalità organizzata (art. 266 co. 2-*bis*). Qui -vien da dire - la legge presume in via assoluta la <<continuità della condotta criminosa>>.

È il caso di ricordare al riguardo che la sentenza con la quale le sezioni unite della Corte di cassazione hanno considerato legittimo l'uso di captatori informatici a fini di intercettazione ambientale riguarda proprio un caso di <<criminalità organizzata>>. Espressione da intendere nel senso (per l'appunto, vago e indefinito, in quanto privo di più precisi riferimenti a fattispecie incriminatrici) di cui all'art. 13 d. l. n. 152 del 1991. In simile vicenda, la Corte di Cassazione si è limitata a considerare legittimo l'uso del captatore informatico, ravvisandovi un semplice mezzo di intercettazione ambientale, non dissimile e, per così dire, fungibile rispetto all'uso di 'cimici' o microspie. La novella del 2017 - segnala l'Autore richiamato - produce nell'area della cd. criminalità organizzata una singolare diversificazione (a seconda del mezzo usato) fra intercettazioni ambientali: quelle realizzate con captatore informatico possono essere effettuate in ambito domiciliare esclusivamente per accertare uno dei reati inclusi negli elenchi di cui all'art. 51, co. 3-*bis* e 5-*quater* (come impone il co. 2-*bis* dell'art. 266); quelle operate con 'cimici' e microspie possono, invece, essere effettuate per accertare un qualsiasi reato di cd. criminalità organizzata, secondo la più evanescente formula testuale dell'art. 13 d.l. 152 del 1991.

Inoltre, si è appunto inteso introdurre una disciplina particolare per i delitti contro la pubblica amministrazione puniti con sanzione detentiva non inferio-

⁸ Sul tema della utilizzabilità dei risultati delle intercettazioni a mezzo *trojan* per reato diverso v. Sez. un., 28 novembre 2019, n. 51 (del 2020), Cavallo, che hanno affermato il seguente principio di diritto: "Il divieto di cui all'art. 270 cod. pen. di utilizzazione dei risultati di intercettazioni di conversazioni in procedimenti diversi da quelli per i quali siano state autorizzate le intercettazioni - salvo che risultino indispensabili per l'accertamento di delitti per i quali è obbligatorio l'arresto in flagranza - non opera con riferimento ai risultati relativi a reati che risultino connessi ex art. 12 cod. proc. pen. a quelli in relazione ai quali l'autorizzazione era stata *ab origine* disposta, sempreché rientrino nei limiti di ammissibilità previsti dalla legge".

V. anche SANTALUCIA, *Il diritto alla riservatezza nella nuova disciplina delle intercettazioni*, Note a margine del d. l. n. 161 del 2019, in *Sistema pen.*, 2020, n. 1, 58.

re a cinque anni (art. 6 d.lgs n. 216 del 2017). Per il loro accertamento sono ammesse le ordinarie intercettazioni, sia telefoniche che ambientali, secondo il regime <<semplificato>> regolato dal citato art. 13 d.l. n. 152 del 1991. Il primo comma dell'art. 6 attua, invero, una sostanziale equiparazione dei delitti di corruzione ai reati di cd. criminalità organizzata, secondo una tendenza (già affermata in altri contesti normativi) volta ad agevolare l'attività di prevenzione e contrasto di reati reputati particolarmente pericolosi per la <<sicurezza-stabilità sociale>>. E il 2° co. (antecedentemente all'avvento della l. n. 3 del 2019) stabilisce, poi, che per l'accertamento di simili reati le intercettazioni ambientali con captatore non possano essere effettuate nel domicilio privato, salvo che vi sia motivo di ritenere che in quei luoghi sia in corso di svolgimento l'attività criminosa.

Altre differenze - precisa il medesimo Autore - caratterizzano la disciplina dei due tipi di intercettazione ambientale nei procedimenti di cd. criminalità organizzata (*lato o stricto sensu*). Quelle - per così dire tradizionali, eseguite con 'cimici' o microspie - possono essere disposte sulla scorta di "sufficienti indizi di reato" e hanno durata di quaranta giorni prorogabili. Diversamente, quelle eseguite con captatori informatici ricadono nella disciplina generale delle intercettazioni, sicché, quand'anche disposte nel procedimento per l'accertamento di delitti inclusi nelle liste dell'art. 51, co. 3-bis e 5-quater, sono soggette al ricorrere dei presupposti indicati nell'art. 267 cpp: si esigono "gravi indizi di reato" e possono svilupparsi in un arco temporale massimo di quindici giorni, salvo l'autorizzazione di proroghe.

Le segnalate differenze trovano evidentemente la loro ragion d'essere nel particolare apprezzamento riconosciuto dal legislatore ai diritti individuali compressi e sacrificati dall'uso del captatore informatico: l'uso di tale mezzo è, evidentemente, considerato più invasivo di altri, quali le 'cimici' o le microspie.

Tale rilievo si rivela importante per impostare e risolvere il problema del rapporto fra le due modalità di intercettazione: entrambe mirano allo stesso risultato (acquisire le comunicazioni di due o più persone in un ambiente determinato), ma ciò realizzano con diversa tecnologia. Il rilievo della maggior invasività di uno degli strumenti rispetto all'altro pone al giudice il compito di vagliare la richiesta del pubblico ministero ex art. 266, co. 2-bis cpp, alla luce del <<principio di proporzionalità>> e, precisamente, alla luce di quel <<criterio di necessità>> che di tale principio costituisce una delle componenti strutturali.

L'assunto trova conferma testuale nella formulazione dell'art. 267, 1° co. e,

precisamente, nella parte introdotta dal d.lgs n. 216 del 2017. Se, invero, per entrambe le forme di intercettazione è comune presupposto di legittimazione la “assoluta indispensabilità”, per la sola captazione informatica si è inteso imporre al giudice che autorizza di indicare “le ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini”.

Si è, dunque, in presenza - osserva criticamente Orlandi - di due distinte manifestazioni del principio di proporzionalità: *sub specie necessitatis* la “assoluta indispensabilità” menzionata nell’art. 267, 1° co., seconda parte serve a escludere il ricorso all’intercettazione quando altri mezzi di prova, in concreto meno invasivi (ad esempio, acquisizione di documenti, audizione di testimoni), siano disponibili. Diversamente, il requisito-limite della “necessità” di cui parla la terza parte del 2° co., è funzionale a rendere <<eccezionale>> il ricorso all’intercettazione ambientale tramite captatore informatico rispetto a quella eseguita con cimici o microspie. In altre parole, l’autorizzazione all’uso investigativo del cd. *trojan horse* dovrà essere rilasciato solo quando si dimostri che l’intercettazione ambientale con altri mezzi, meno invasivi, si riveli insufficiente a raggiungere lo scopo.

Usi diversi da quelli espressamente regolati nell’art. 266, 2° co. e *2-bis* co., non sono in ogni caso ammessi. E ciò proprio perché simili <<usi>> limitano, appunto, un diritto fondamentale della persona. Le <<perquisizioni a distanza>>, il <<monitoraggio del comportamento>> di chi ha in uso il dispositivo sorvegliato, l’<<acquisizione-sequestro>> di documenti ovvero immagini, non infrequenti nella prassi, costituiscono la riprova di quanto *poco* la nostra cultura giuridico-processuale penale sia sensibile ai diritti fondamentali della persona e di quanto sia incline a trascurare quel principio di proporzionalità, posto al servizio di un ideale bilanciamento fra esigenze individuali ed efficienza investigativa.

Punto questo delicatissimo, per la ragione che la giurisprudenza - analogamente a quanto avvenuto in altri settori - potrebbe adagiarsi sull’idea che il (solo ritenuto) <<vuoto normativo>> implichi assenza di qualsiasi divieto nell’uso del captatore come mezzo di controllo o di perquisizione-sequestro a distanza. Non è consentito ricorrere con superficiale facilità alla formula *passé-partout* della <<prova atipica>> per far entrare nel processo <<materiale spurio>>, in quanto acquisito in violazione di un diritto individuale la cui (pur possibile) <<compressione>> non è puntualmente disciplinata dalla legge.

4. *L’estensione dell’operatività del captatore informatico ai delitti dei pubblici ufficiali contro la P.A. La posizione della dottrina circa la (non) immediata*

applicabilità della legge cd. “Spazzacorrotti”. Con il recente intervento della cd. “Spazzacorrotti”, la disciplina derogatoria è stata ulteriormente ampliata: l’impiego del captatore nei luoghi di privata dimora e assimilati è ora <<sempre possibile>> - pur in assenza di motivi che portino a ritenere che sia qui in corso di svolgimento l’attività criminosa - anche per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni (ai sensi dell’art. 4 cpp.).

Al riguardo si è, innanzitutto, osservato che “appare evidente...l’appiattimento della disciplina delle intercettazioni nei procedimenti per i più gravi delitti contro la pubblica amministrazione sul modulo stabilito per i procedimenti aventi ad oggetto i reati di criminalità organizzata o ad essi equiparati. Di tal guisa, è lecito concludere che la recente normativa conduce ad una disciplina delle intercettazioni che non rispetta il ragionato bilanciamento tra esigenze investigative e diritti fondamentali”. Non può, invero, difettare un rapporto di proporzionalità diretta - si precisa - fra il grado di intrusività della specifica misura e il livello di intensità delle garanzie legali, attraverso un equilibrato bilanciamento fra contrapposti <<valori>> di rilevanza costituzionale.

Sotto un diverso profilo - aspetto che qui maggiormente interessa - va segnalato che la legge n. 3 del 2019 - che ha, appunto, reso <<sempre possibili>> le intercettazioni ambientali con il captatore informatico per i più gravi delitti dei pubblici ufficiali contro la P.A. - ha *al contempo abrogato* la norma che (nell’estendere il ricorso alle intercettazioni cd. antimafia anche a simili delitti) ne vietava l’effettuazione nei luoghi di privata dimora in assenza di motivi per ritenere in corso attività criminosa. Ora, sul punto, la dottrina ha, unanimemente, inteso affermare che, comunque, “la novità qui descritta [pur essendo la legge in esame in vigore dal 31 gennaio 2019] opererà solo in relazione <<alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 luglio 2019, visto che così recita la normativa transitoria del d.l.vo 216/17, [fonte normativa questa] che ha introdotto la disciplina derogatoria su cui si è innestata la novella in commento”⁹.

Invero -si rileva - “la piena operatività della disposizione è posticipata per

⁹ TABASCO, *Intercettazioni, a mezzo di captatore informatico, nei procedimenti per delitti contro la pubblica amministrazione*, in *La legge anticorruzione 9 gennaio 2019 n. 3, Aggiornata alla l. 28 giugno 2019 n. 58*, a cura di M. del Tufo, Torino, 2019, 153 s.

Segnala il rischio di un’estensione dell’ambito applicativo del captatore informatico a seguito della specificazione che i delitti contro la P.A. sono anche quelli commessi dagli <<incaricati di pubblico servizio>> SANTALUCIA, *op. cit.*, 58.

¹⁰ NIGRO, *L’ampliamento delle ipotesi di impiego del <<trojan horse>>*, in *discrimem focus*, 6 marzo 2019.

effetto dell'ulteriore rinvio operato dal decreto sicurezza *bis* [d. l. 14 giugno 2019, n. 53 in vigore dal 15 giugno 2019], per cui la disciplina si applica alle operazioni di intercettazione relative a provvedimenti autorizzativi emessi dopo il 31 dicembre 2019¹¹.

Ed in tal senso si precisa: “Ebbene, rispetto allo stato dell'arte sopra descritto l'art. 1, co.4, lett. a, L. 9 gennaio 2019 n. 3 opera su due piani distinti. Da un lato, modifica ulteriormente l'art. 266, co.2 bis, c.p.p., consentendo l'utilizzo del captatore informatico quando si procede per i più gravi delitti dei pubblici ufficiali contro la pubblica amministrazione. Tale modifica, tuttavia, riguarda una norma non ancora vigente, con la conseguenza che, pur essendo già stata approvata, l'effettiva efficacia di tale disposizione è di fatto prorogata al 1° gennaio 2019 (data di entrata in vigore dell'art. 266, co. 2-*bis*, c.p.p.)...”¹².

5. *Il diverso orientamento delle Sezioni unite civili.* Giungono, invece, a diverse conclusioni circa il termine iniziale di operatività della legge cd. <<Spazzacorrotti>> in materia di intercettazioni ambientali a mezzo captatore informatico per i più gravi delitti dei pubblici ufficiali contro la P.A. (31 gennaio 2019 ovvero 31 luglio 2019-1gennaio 2020) le Sezioni unite civili che con sentenza n. 741 del 2020 ud. 3 dicembre 2020 - dep. 15 gennaio 2020, P. c. Ministero della giustizia), ricostruito il quadro normativo di riferimento, fissano l'entrata in vigore della l. 9 gennaio 2019 n. 3 nella parte qui d'interesse nel “decimoquinto giorno dalla pubblicazione della legge sulla G.U. avvenuta il 16 gennaio 2019”.

A tal fine si osserva innanzitutto:

“*Per i reati per i quali è ammessa l'intercettazione di conversazioni o comunicazioni (art. 266, co. 1, c.p.p.), intercettazione di comunicazioni tra presenti se si svolge in luoghi di privata dimora (art. 614 c.p.) è consentita “solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa” (art. 266, co. 2, c.p.p.)*

Una disciplina espressamente qualificata derogatoria fu introdotta dalla legislazione in materia di criminalità organizzata e mafiosa emanata nel biennio 1991-1992.

L'art. 13 d.l. 13 maggio 1991, n. 152, convertito con modificazioni in legge 12

¹¹ BENE, *op. cit.*, 4. Analogamente ORLANDI, *op. cit.*, 554.

¹² LA TORRE, *Il captatore informatico dopo la legge cd. <<Spazzacorrotti>>*, in *Dir. pen. processo*, 2019, n. 5, 651. Sembra orientato alla medesima conclusione SANTALUCIA, *op. cit.*, 57, secondo cui “le modifiche apportate dalla legge cd. spazzacorrotti - con ogni probabilità mai divenute operative perché innestate nel corpo di disposizioni oggetto delle reiterate previsioni di rinvio, nel tempo, dell'acquisto di efficacia...”.

luglio 1991, n. 203, ha stabilito che per disporre le operazioni previste dall'articolo 266 c.p.p., quando l'intercettazione è necessaria per lo svolgimento delle indagini in relazione ad un delitto di criminalità organizzata o di minaccia col mezzo del telefono, fossero necessari solo "sufficienti indizi". La norma inoltre per questo tipo di reati ha dilatato i termini di durata massima di intercettazione (quaranta giorni, in luogo di quindici), nonché delle possibili proroghe (venti giorni, in luogo di quindici).

Il contenuto dell'art. 13 è stato integrato da una disposizione del d.l. 8 giugno 1992 n. 306, in materia di criminalità mafiosa, emanato a seguito della strage di Capaci e convertito con modificazioni nella legge 7 agosto 1992. Il legislatore ha stabilito che "quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo ad un delitto di criminalità organizzata e che avvenga nei luoghi indicati all'art. 614 c.p., l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa".

Con la sentenza n. 26886 del 28 aprile 2016, Scurato, le Sezioni unite Penali hanno affrontato il problema dell'intercettazione di comunicazioni tra presenti mediante l'installazione di un captatore informatico in un dispositivo elettronico, rilevando che, quando si autorizza l'utilizzazione di questo strumento, si deve necessariamente prescindere dall'indicazione dei luoghi in cui la captazione deve avvenire, posto che è impossibile, per tale mezzo di indagine, una preventiva individuazione ed indicazione dei luoghi di interesse, data la natura itinerante dello strumento di indagine da utilizzare.

Le Sezioni unite hanno richiamato l'art. 13 come integrato nel 1992, affermando che l'intercettazione mediante captatore informatico è ammissibile nei soli procedimenti per i delitti di criminalità organizzata di cui all'art. 13 del d.l. 152 del 1991, perché tale norma consente la captazione anche nei luoghi di privata dimora, senza necessità di preventiva individuazione ed indicazione di tali luoghi e prescindendo dalla dimostrazione che siano sedi di attività criminosa in atto.

La medesima sentenza ha anche precisato: "In tema di intercettazioni di conversazioni o comunicazioni, ai fini dell'applicazione della disciplina derogatoria delle norme codicistiche prevista dall'art. 13 d.l. 152/1991, per procedimenti relativi a delitti di criminalità organizzata devono intendersi quelli elencati nell'art. 51, co. 3-bis e 3-quater, c.p.p., nonché quelli comunque facenti capo ad una associazione per delinquere, con esclusione del mero concorso di persone nel reato".

Ciò preliminarmente chiarito, si rileva:

“In tale contesto, è stato emanato il d.lgs. 29 dicembre 2017, n. 2016 (c.d. decreto Orlando), il cui art. 4 ha modificato il comma 2 dell’art. 266 c.p.p., inserendo le seguenti parole: “che può essere eseguita anche mediante l’inserimento di un captatore informatico su dispositivo elettronico portatile”. Ha poi aggiunto un comma 2-bis alla disposizione codicistica, in forza del quale: “L’intercettazione di comunicazioni o conversazioni tra presenti mediante inserimento di captatore informatico su dispositivo elettronico portatile è sempre consentita nei procedimenti di cui all’art. 51, co. 3-bis e 3-quater”. La norma codifica quindi il quadro normativo preesistente ricostruito dalla Sezioni unite nel 2016.

Il legislatore del 2017 è, anche, intervenuto in materia di reati dei pubblici ufficiali contro la pubblica amministrazione. L’art. 6 del decreto legislativo 216, al primo comma, ha, infatti, esteso ai procedimenti per i delitti dei pubblici ufficiali contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni, le disposizioni di cui all’art. 13 del d.l. 1991. L’estensione però non è stata integrale perché il secondo comma ha stabilito che, contrariamente a quanto previsto per i reati di criminalità organizzata, con riferimento ai reati contro la p.a. “L’intercettazione di comunicazioni tra presenti nei luoghi indicati dall’art. 614 c.p. non può essere eseguita mediante l’inserimento di un captatore informatico su dispositivo elettronico portatile quando non vi è ritenere che ivi si stia svolgendo attività criminosa”.

Il decreto legislativo contiene una disciplina transitoria, dettata dall’art. 9, che postone (con termine più volte prorogato) l’entrata in vigore di alcune norme (precisamente artt. 2, 3, 4, 5 e 7) tra le quali non figura, però, l’art. 6, che, come si è visto, ha consentito l’uso del captatore informatico per le intercettazioni tra presenti nelle indagini per i reati dei pubblici ufficiali contro la p. a., disposizione che è dunque entrata in vigore il 26.1.2018, dopo lo spirare dell’ordinario termine dalla pubblicazione del decreto, avvenuta l’11.1.2018”.

E venendo finalmente all’esame delle modifiche introdotte dalla legge cd. <<Spazzacorrotti>> nella materia qui in esame, si afferma:

“Il legislatore è tornato sui reati nei confronti della p.a. con la legge 9 gennaio 2019, n. 3, apportando anche alcune modifiche alla normativa sulle intercettazioni. In particolare, il terzo comma dell’art. 1, ha abrogato il secondo comma dell’art. 6 del d. lgs. n. 216 del 2017: di conseguenza, è venuta meno la restrizione dell’uso del captatore informatico nei luoghi indicati dall’art. 614 c.p. In questi luoghi, pertanto, l’intercettazione può essere eseguita anche se non vi è motivo di ritenere che vi si stia svolgendo attività criminosa.

Il richiamo del primo comma dell'art. 6 all'art. 13 d.l. 152 del 1991 è divenuto così integrale e non vi è diversità sul punto tra la disciplina in materia di intercettazioni per la criminalità organizzata e quella per i reati più gravi contro la pubblica amministrazione.

Questa parte della legge 9 gennaio 2019, n. 3 è entrata in vigore il decimoquinto giorno dalla pubblicazione della legge sulla G.U. avvenuta il 16 gennaio 2019. Una controprova è costituita dal fatto che, invece, con riferimento ad altre disposizioni della medesima legge, il legislatore ha differito l'entrata in vigore al 1° gennaio 2020.

Il ricorrente sostiene, anche in seno alla memoria, che, essendo stata differita la modifica dell'art. 266 c.p.p. operata dall'art. 4 del decreto legislativo 216, “ne consegue che, in relazione alle intercettazioni mediante captatore informatico, neanche la disciplina introdotta dalla legge 3/2019 può trovare immediata applicazione, poiché ‘subisce’ il differimento previsto per le disposizioni della legge Orlando, rispetto alle quali non ha autonomia propria”.

La tesi è infondata perché, come si è visto, la possibilità di utilizzare il captatore informatico preesiste e prescinde dalla modifica del testo codicistico operata dall'art. 4 del d. lgs. 216 del 2017, e deriva direttamente, come hanno precisato le Sezioni Unite Penali, dall'art. 13 del d.l. 152 del 1991, norma il cui ambito di efficacia è stato esteso dall'art. 6 del d. lgs. 261 del 2017 anche ai più gravi reati contro la p.a. L'entrata in vigore di quest'ultima norma non è stata rinviata, così come è entrata in vigore secondo i termini ordinari la previsione della legge 3 del 2019 che ne ha eliso il secondo comma. Pertanto, all'epoca dei fatti oggetto del presente procedimento disciplinare era in vigore la disciplina che autorizza l'utilizzatore del captatore informatico anche per i reati più gravi contro la pubblica amministrazione, senza la delimitazione originariamente prevista dal secondo comma dell'art. 6 del d. lgs. 216 del 2017”.

5. Osservazioni critiche. Ora, in realtà, il secondo comma dell'art. 6 d. lgs. n. 216 del 2017 -oggi abrogato dalla legge cd. <<Spazzacorrotti>>- ha sì ad oggetto l'uso del captatore informatico nei reati in questione, “ma -all'evidenza- pone una regola che limita il potere investigativo, vietando l'intrusione informatica su dispositivi portatili localizzati nel domicilio privato, quando non vi sia motivo di ritenere che lì si svolga l'attività criminosa presa di mira. Si tratta, pertanto, di regola priva di vita autonoma [forse, più chiaramente, regola meramente integratrice] destinata necessariamente a combinarsi, precisandola, con la norma che ammette -in linea generale- l'uso dei captatori informatici: l'art. 266 co. 2 ultima parte. E non c'è dubbio che l'entrata in vigore di

quest'ultima cade" a fine luglio 2019 [termine poi prorogato al 31 dicembre 2019]¹³.

Non ancora in vigore (*rectius*, non ancora normativamente definita) la disciplina dell'uso del captatore informatico per i delitti di criminalità organizzata e dei delitti dei pubblici ufficiali contro la P.A., il ricorso a tale <<pratica investigativa>> risulterebbe realizzabile nella lettura del S.C., operando una sorta di *mix* tra giurisprudenza creativa (i termini della sentenza Scurato che nel 2016 ha inteso <<anticipare>> una riforma *in itinere*; riforma che oggi prefigura contenuti, almeno in parte, diversi) ed una fonte normativa che ha sì già abrogato l'art. 6, 2° co., d. lgs. n. 216 del 2017, ma che nondimeno ancora attende l'entrata in vigore degli artt. 266 e 267 cpp - disposizioni, per così dire, <<portanti>> - che dovranno disciplinare il processo autorizzativo della medesima <<pratica investigativa>>.

Tema, più in generale, della successione di leggi in materia sul quale è dato riportare il pensiero di autorevole dottrina: "Resta da dire della successione di leggi riguardanti l'uso del captatore informatico. Il giorno di passaggio da un regime all'altro è -come ricordato- il 26 luglio 2019, quale che sia il delitto da accertare. Le misure disposte prima di tale data sono soggette alla regolamentazione previgente, che non regolava *ad hoc* tale modalità di intercettazione. *Circola l'opinione*¹⁴ che la normativa previgente fosse quella stabilita in via giurisprudenziale, in particolare dalla presa di posizione della Corte di cassazione a sezioni unite nella già citata sentenza Scurato...A ben vedere, però, la giurisprudenza di legittimità si è limitata a trarre dalla normativa preesistente una conclusione assai plausibile anche in tema di uso (a fini di intercettazione di comunicazioni) del captatore informatico. L'art. 266-*bis* c.p.p., nella versione in vigore dal lontano 1993, ammetteva (e tutt'ora ammette) <<intercettazioni telematiche>>. Difficile negare che quel generico aggettivo, "telematiche", fosse riferibile anche alle intercettazioni informatiche. Ovviamente, nel 1993 non si pensava all'evoluzione del *world wide web* e alla capillare diffusione di dispositivi portatili verificatasi in misura imponente nell'ultimo decennio. Resta però il rilievo che la qualifica di <<telematiche>> ben poteva adattarsi alla comparsa delle nuove tecnologie informatiche: nel che si può ravvisare non un caso di creatività giurisprudenziale, quanto piuttosto la -per l'appunto- plausibile interpretazione di una parola (<<telematiche>>) adattata

¹³ ORLANDI, *op. cit.*, 554

¹⁴ Il riferimento è a GAMBARDELLA, *La disciplina transitoria del captatore informatico*, in *Nuove norme in tema di intercettazioni. Tutela della riservatezza, garanzie difensive e nuove tecnologie informatiche*, a cura di Giostra, Orlandi, 2018, 277.

allo sviluppo tecnologico. Indubbiamente, il captatore informatico consente, di fatto, usi che vanno ben oltre l'intercettazione di comunicazioni interpersonali ed è pertanto opportuno che lo si regolamenti a parte, tenendo conto dei molteplici interessi e diritti individuali coinvolti nell'operazione captativa. *E questo è compito del legislatore*, mentre si deve ammettere che la Corte di cassazione –in particolare con la sentenza Scurato– si è limitata a considerare coperta dalla disciplina previgente (principalmente dall'art. 266-*bis*) questa nuova modalità di intercettazione. Per quanto ci riguarda, quindi, *la successione di leggi si realizza fra la previgente, generica previsione incentrata nel citato art. 266-bis e la riforma del 2017*¹⁵.

Sembra, pertanto, di poter concludere coll'affermare che la legge n. 3 del 2019 (cd. <<Spazzacorrotti>>) è entrata interamente in vigore senza prevedere alcuna disciplina transitoria *in subiecta materia*, né esplicita modifica e/o abrogazione dell'art. 9 della riforma <<Orlando>>. Simile fonte normativa ha apportato modifiche agli artt. 266 e 267 c.p.p., *ma tali innovazioni riguardano non già il testo originario delle disposizioni codicistiche, bensì il testo risultante dalle modifiche della riforma Orlando, non ancora vigente*.

Ne consegue, in relazione alle intercettazioni mediante captatore informatico, che neanche la disciplina introdotta dalla legge n. 3 del 2019 in materia di delitti dei pubblici ufficiali contro la P.A. può trovare immediata applicazione, poiché <<subisce>> il differimento previsto per le disposizioni della legge Orlando, *rispetto alle quali non ha autonomia propria*.

D'altra parte, il d.l. *sicurezza-bis* dello scorso 14 giugno 2019, intervenendo sulla disciplina transitoria dell'art. 9 riforma Orlando, esclude definitivamente l'erronea interpretazione della implicita abrogazione della stessa proroga *ex art. 9 <<riforma Orlando>>* ad opera della "Spazzacorrotti" (che nulla prevede al riguardo): il d.l. *sicurezza bis*, avendo ad oggetto proprio l'art. 9 <<riforma Orlando>> e disponendo l'ulteriore proroga dell'entrata in vigore della nuova disciplina in tema di intercettazioni al 31 dicembre 2019, elimina qualsiasi dubbio sulla <<attuale vigenza>> della disciplina transitoria in questione.

Peraltro, analizzando la stessa successione dei vari interventi –dalla riforma Orlando al recentissimo d.l. *sicurezza bis*– non può non concludersi che il nuovo termine di proroga (stabilito dal d.l. *sicurezza bis* al 31 dicembre 2019) debba oggi applicarsi necessariamente alle attuali versioni degli artt. 266 e 267 c.p.p., per come modificati a seguito sia dalla riforma <<Orlando>>, sia dalla

¹⁵ Così ORLANDI, *op. cit.*, 555 (corsivi di chi scrive).

cd. <<Spazzacorrotti>> (che li estende ai delitti dei pubblici ufficiali contro la P.A.).

La cronologia degli interventi elimina, infatti, qualsiasi dubbio sull'estensione della disciplina transitoria dell'art. 9 riforma Orlando, anche all'uso del captatore nei delitti del pubblico funzionario contro la P.A.

Come noto, in questi ultimi giorni, il giudice delle leggi ha ritenuto incompatibile con il principio di legalità della pena l'applicazione retroattiva delle modifiche peggiorative della disciplina delle misure alternative alla detenzione (nonché della liberazione condizionale e del divieto di sospensione dell'ordine di carcerazione successivo alla sentenza di condanna), modifiche introdotte dalla legge cd <<Spazzacorrotti>>: si è inteso riconoscere "costituzionalmente illegittima", invero, "la costante interpretazione giurisprudenziale" in argomento, interpretazione - rileva la Corte Costituzionale - seguita "anche con riferimento alla legge n. 3 del 2019"¹⁶.

Si auspica, dunque, che un qualcosa di simile possa avvenire anche in tema di immediata applicabilità della novella sull'utilizzazione del captatore informatico in materia di delitti dei pubblici ufficiali contro la P.A., appalesandosi davvero improbabile -anche in ragione dell'improprio quanto strumentale accostamento di simili delitti ai reati di criminalità organizzata- un *revirement* della S.C. rispetto alla propria erronea, e già consolidata, lettura.

¹⁶ Corte cost. Comunicato del 12 febbraio 2020: " ... Secondo la Corte ... l'applicazione retroattiva di una disciplina che comporta una radicale trasformazione della natura della pena e della sua incidenza sulla libertà personale, rispetto a quella prevista al momento del reato, è incompatibile con il principio di legalità delle pene, sancito dall'art. 25, secondo comma, della Costituzione".

Sui limiti e, in particolare, sull'oggetto del controllo di costituzionalità v. in generale, il recente lavoro di MANES-NAPOLEONI, *La legge penale illegittima, Metodo, itinerari e limiti della questione di costituzionalità in materia penale*, Torino, 2019.