

SP

SISTEMA
PENALE

FASCICOLO

10/2020

COMITATO EDITORIALE Giuseppe Amarelli, Roberto Bartoli, Hervé Belluta, Michele Caianiello, Massimo Ceresa-Gastaldo, Adolfo Ceretti, Cristiano Cupelli, Francesco D'Alessandro, Angela Della Bella, Gian Paolo Demuro, Emilio Dolcini, Novella Galantini, Mitja Gialuz, Glauco Giostra, Antonio Gullo, Stefano Manacorda, Vittorio Manes, Luca Masera, Anna Maria Maugeri, Melissa Miedico, Vincenzo Mongillo, Francesco Mucciarelli, Claudia Pecorella, Marco Pelissero, Lucia Risicato, Marco Scoletta, Carlo Sotis, Costantino Visconti

COMITATO SCIENTIFICO Alberto Alessandri, Silvia Allegrezza, Ennio Amodio, Gastone Andreazza, Ercole Aprile, Giuliano Balbi, Marta Bargis, Fabio Basile, Alessandra Bassi, Teresa Bene, Carlo Benussi, Alessandro Bernardi, Marta Bertolino, Rocco Blaiotta, Manfredi Bontempelli, Renato Bricchetti, David Brunelli, Carlo Brusco, Silvia Buzzelli, Alberto Cadoppi, Lucio Camaldo, Stefano Canestrari, Giovanni Canzio, Francesco Caprioli, Matteo Caputo, Fabio Salvatore Cassibba, Donato Castronuovo, Elena Maria Catalano, Mauro Catenacci, Antonio Cavaliere, Francesco Centonze, Federico Consulich, Stefano Corbetta, Roberto Cornelli, Fabrizio D'Arcangelo, Marcello Daniele, Gaetano De Amicis, Cristina De Maglie, Alberto De Vita, Ombretta Di Giovine, Gabriella Di Paolo, Giandomenico Dodaro, Massimo Donini, Salvatore Dovere, Tomaso Emilio Epidendio, Luciano Eusebi, Riccardo Ferrante, Giovanni Fiandaca, Giorgio Fidelbo, Carlo Florio, Roberto Flor, Luigi Foffani, Désirée Fondaroli, Gabriele Fornasari, Gabrio Forti, Piero Gaeta, Marco Gambardella, Alberto Gargani, Loredana Garlati, Giovanni Grasso, Giulio Illuminati, Gaetano Insolera, Roberto E. Kistoris, Sergio Lorusso, Ernesto Lupo, Raffaello Magi, Vincenzo Maiello, Grazia Mannozi, Marco Mantovani, Marco Mantovani, Luca Marafioti, Enrico Marzaduri, Maria Novella Masullo, Oliviero Mazza, Claudia Mazzucato, Alessandro Melchionda, Chantal Meloni, Vincenzo Militello, Andrea Montagni, Gaetana Morgante, Lorenzo Natali, Renzo Orlandi, Luigi Orsi, Francesco Palazzo, Carlo Enrico Paliero, Lucia Parlato, Annamaria Peccioli, Chiara Perini, Carlo Piergallini, Paolo Pisa, Luca Pistorelli, Daniele Piva, Oreste Pollicino, Domenico Pulitanò, Serena Quattrocchio, Tommaso Rafaraci, Paolo Renon, Maurizio Romanelli, Gioacchino Romeo, Alessandra Rossi, Carlo Ruga Riva, Francesca Ruggieri, Elisa Scaroina, Laura Scomparin, Nicola Selvaggi, Sergio Seminara, Paola Severino, Rosaria Sicurella, Piero Silvestri, Fabrizio Siracusano, Andrea Francesco Tripodi, Giulio Ubertis, Antonio Vallini, Gianluca Varraso, Vito Velluzzi, Paolo Veneziani, Francesco Viganò, Daniela Vigoni, Francesco Zacchè, Stefano Zirulia

REDAZIONE Francesco Lazzeri (coordinatore), Enrico Andolfatto, Enrico Basile, Silvia Bernardi, Carlo Bray, Pietro Chiaraviglio, Stefano Finocchiaro, Beatrice Fragasso, Alessandra Galluccio, Cecilia Pagella, Tommaso Trinchera, Maria Chiara Ubiali

Sistema penale (SP) è una rivista *online*, aggiornata quotidianamente e fascicolata mensilmente, ad accesso libero, pubblicata dal 18 novembre 2019.

La *Rivista*, realizzata con la collaborazione scientifica dell'Università degli Studi di Milano e dell'Università Bocconi di Milano, è edita da Progetto giustizia penale, associazione senza fine di lucro con sede presso il Dipartimento di Scienze Giuridiche "C. Beccaria" dell'Università degli Studi di Milano, dove pure hanno sede la direzione e la redazione centrale. Tutte le collaborazioni organizzative ed editoriali sono a titolo gratuito e agli autori non sono imposti costi di elaborazione e pubblicazione.

La *Rivista* si uniforma agli standard internazionali definiti dal *Committee on Publication Ethics* (COPE) e fa proprie le relative linee guida.

I materiali pubblicati su *Sistema Penale* sono oggetto di licenza CC BY-NC-ND 4.00 International. Il lettore può riprodurli e condividerli, in tutto o in parte, con ogni mezzo di comunicazione e segnalazione anche tramite collegamento ipertestuale, con qualsiasi mezzo, supporto e formato, per qualsiasi scopo lecito e non commerciale, conservando l'indicazione del nome dell'autore, del titolo del contributo, della fonte, del logo e del formato grafico originale (salve le modifiche tecnicamente indispensabili).

Il testo completo della licenza è consultabile su <https://creativecommons.org/licenses/by-nc-nd/4.0/>.

Peer review I contributi che la direzione ritiene di destinare alla sezione "Articoli" del fascicolo mensile sono inviati a un revisore, individuato secondo criteri di rotazione tra i membri del Comitato scientifico, composto da esperti esterni alla direzione e al comitato editoriale. La scelta del revisore è effettuata garantendo l'assenza di conflitti di interesse. I contributi sono inviati ai revisori in forma anonima. La direzione, tramite la redazione, comunica all'autore l'esito della valutazione, garantendo l'anonimato dei revisori. Se la valutazione è positiva, il contributo è pubblicato. Se il revisore raccomanda modifiche, il contributo è pubblicato previa revisione dell'autore, in base ai commenti ricevuti, e verifica del loro accoglimento da parte della direzione. Il contributo non è pubblicato se il revisore esprime parere negativo alla pubblicazione. La direzione si riserva la facoltà di pubblicare nella sezione "Altri contributi" una selezione di contributi diversi dagli articoli, non previamente sottoposti alla procedura di *peer review*. Di ciò è data notizia nella prima pagina della relativa sezione.

Di tutte le operazioni compiute nella procedura di *peer review* è conservata idonea documentazione presso la redazione.

Modalità di citazione Per la citazione dei contributi presenti nei fascicoli di *Sistema penale*, si consiglia di utilizzare la forma di seguito esemplificata: N. COGNOME, *Titolo del contributo*, in *Sist. pen. (o SP)*, 1/2020, p. 5 ss.

SONO INUTILIZZABILI I DATI INTERCETTATI A MEZZO DI CAPTATORE INFORMATICO AL DI FUORI DEI LUOGHI CONSENTITI

Nota a [Cass., Sez. I, sent. 25 giugno 2019 \(dep. 17 dicembre 2019\),
n. 50972, Pres. Di Tomassi, Est. Cairo](#)

di Mario Griffo

Con un raro pronunciamento in tema di inutilizzabilità delle intercettazioni eseguite attraverso captatore informatico, la Corte di cassazione ha affrontato il problema della tassativa individuazione dei luoghi di svolgimento delle relative attività. In particolare, muovendo dalla “sentenza Scurato”, i giudici di legittimità hanno censurato la prassi investigativa di attivazione del microfono al di fuori dei luoghi di svolgimento della attività delittuosa previamente individuati nel decreto autorizzativo emesso dal giudice procedente. Il dato più significativo, che rende la decisione particolarmente interessante, comunque, dato dal fatto che nel caso specifico le captazioni poi dichiarate inutilizzabili erano state effettuate in luogo pubblico e non già in “luogo di privata dimora”.

SOMMARIO: 1. Il *casus belli*. – 2. Un breve *excursus* disciplinare. – 3. Le modalità intercettive quanto ai “luoghi” ed al “tempo”. – 4. Le declinazioni della prassi. – 5. Le cause di inutilizzabilità. – 6. Riflessioni conclusive.

1. Il *casus belli*.

Quella annotata costituisce sentenza non particolarmente valorizzata dalla ermeneutica corrente probabilmente a causa della cristallizzazione, nella massima, di un principio di diritto alla apparenza scontato: sono inutilizzabili le intercettazioni eseguite attraverso captatore informatico in luoghi diversi da quelli ove si stia svolgendo attività criminosa.

La pronuncia, viceversa, letta nella sua interezza possiede significativo rilievo nella generale economia del dibattito instauratosi in ordine alle potenzialità operative del captatore informatico. Essa, infatti, connette la (in)utilizzabilità dei risultati incamerati tramite *trojan horse*, esclusivamente, alla individuazione del *locus* presidiato dalle guarentigie di cui all’art. 614 c.p.p. nel relativo provvedimento autorizzativo.

Nel caso posto alla attenzione della Corte di legittimità si discuteva, non a caso, di intercettazioni eseguite tramite captatore a mo’ di microspia, con la limitazione che le captazioni non avvenissero in luoghi di privata dimora.

A voler schematizzare, il Giudice per le indagini preliminari (procedente) emetteva due decreti in successione fissando le relative condizioni di applicazione, escludendo i domicili privati dagli ambiti di impiego del captatore.

Tutto questo avrebbe determinato, in ipotesi, la utilizzabilità di alcune intercettazioni di colloqui svoltisi sulla pubblica via in quanto non avvenute in luogo di privata dimora, procedendosi per delitti diversi da quelli di criminalità organizzata.

Al cospetto di un simile quadro, il Giudice di legittimità ha osservato che le intercettazioni per delitti diversi da quelli di criminalità organizzata, non possono essere eseguite nei luoghi di privata dimora, attraverso il captatore informatico, se non vi sia fondato motivo di ritenere che ivi sia in corso attività criminosa. Il captatore, infatti, “accedendo a dispositivi portatili e che hanno possibilità di realizzare ascolti itineranti, non sarà, pertanto, utilizzabile come strumento di impiego delle intercettazioni se non alle anzidette condizioni, giacché la caratteristica degli strumenti stessi condiziona la modalità di autorizzazione e acquisitiva delle conversazioni, oltre a rischiare di esporre ad acquisizioni non conformi al testo di legge, allo stato in vigore...Né risulta possibile una legalizzazione successiva”.

La conclusione impone di tracciare, sia pure per grandi linee, le direttrici lungo le quali si è mosso il legislatore – su *input* della giurisprudenza di legittimità – nel disciplinare le intercettazioni (ambientali) esperibili attraverso captatore informatico.

2. Un breve *excursus* disciplinare.

Come è noto le Sezioni unite della Corte di cassazione, con la “sentenza Scurato”, si sono soffermate sulla possibilità di impiegare, per lo svolgimento delle intercettazioni tra presenti, programmi informatici inseriti a distanza in apparecchi elettronici (smartphone, computer o tablet)¹.

Il nucleo centrale della questione e l’aspetto di maggiore rilevanza della pronuncia hanno interessato il carattere dei dispositivi anzidetti.

Essi seguono ordinariamente l'utilizzatore e ne permettono l'impiego come “microspie”. A ciò si aggiunge la possibilità di sfruttarne il profilo itinerante per effettuare intercettazioni all'interno di domicili con il conseguente rischio di possibili elusioni dei limiti normativamente fissati (attività delittuosa *in itinere*), senza indicazione, *ex ante*, dei luoghi in cui acquisire le informazioni attraverso la captazione delle conversazioni.

Sicché, la anzidetta decisione delle Sezioni unite, dopo una completa ricostruzione degli orientamenti susseguitisi nel tempo, ha ammesso l’uso del particolare strumento informatico laddove si proceda per i delitti di criminalità organizzata (art. 51, commi 3-*bis* e 3-*quater*, c.p.p.), caso in cui troverebbe applicazione il disposto di cui all’art. 13 del d.l. 13 maggio 1991, n. 152, conv. con mod. nella l. 12 luglio

¹ Cass., Sez. Un., 28 aprile 2016, n. 26889, in *C.E.D. Cass.*, n. 266905.

1991, n. 203, che, in deroga all'art. 266 c.p.p., comma 2, ammette le intercettazioni domiciliari anche in difetto di attività delittuosa in corso.

Nelle altre evenienze, e de *iure condito*, avuto riguardo per il quadro normativo all'epoca vigente, per reati diversi da quelli di criminalità organizzata, le intercettazioni, attraverso l'impiego di strumenti portatili e captatori informatici, non sarebbero state ammissibili.

Detto questo, proiettando il ragionamento sul contesto ordinamentale nel quale si è innestata la decisione in commento bisogna, sia pure per sintesi, penetrare le matrici generali che hanno ispirato i più significativi interventi legislativi dell'ultimo triennio.

Le innovazioni hanno interessato, innanzitutto, i commi 2 e 2-*bis* dell'art. 266 c.p.p.

In specie, interpolando il comma 2 della norma anzidetta, si è prevista la possibilità di disporre intercettazioni di comunicazioni tra presenti anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Se tali intercettazioni avvengono in luoghi privati (614 c.p.) esse sono possibili solo se ivi si stia svolgendo attività criminosa.

La previsione circa la "ordinaria" possibilità di procedere con un captatore informatico su dispositivo elettronico portatile è stata introdotta con il d.lgs. 29 dicembre 2017, n. 216 [art. 4, comma 1, lett. a), n. 1)].

In via derogatoria, comunque, si è statuito – è bene specificarlo – che l'intercettazione delle conversazioni tra presenti a mezzo captatore e su dispositivo portatile è consentita per i delitti di criminalità organizzata nonché per quelli dei pubblici ufficiali contro la pubblica amministrazione puniti con pena non inferiore a cinque anni determinata ai sensi dell'art. 4 c.p.p., senza ulteriori condizioni.

Insomma, anche per i citati delitti dei pubblici ufficiali contro la pubblica amministrazione si applica, per effetto del d.lgs. n. 216 del 2017, la disciplina del d.l. 13 maggio 1991, n. 152, contemplata per i reati di criminalità organizzata.

Al cospetto di tale quadro normativo, il "successivo" d.l. 30 dicembre del 2019, n. 161 (convertito con modificazioni dalla l. 28 febbraio 2020, n. 7) ha attuato una vera e propria controriforma in materia².

Il primo elemento significativo in tale direzione è rinvenibile nel riconoscimento per tutti i reati ricompresi nella previsione di cui all'art. 266 c.p.p. dell'uso del captatore informatico su dispositivo elettronico portatile³.

² Per una prima lettura critica del provvedimento, A. SCALFATI, *Intercettazioni, spirito autoritario, propaganda e norme inutili*, in *Arch. pen web*, 2020, 1, p. 1 ss.

³ La disciplina dell'impiego del captatore informatico nel processo penale viene introdotta ad opera degli artt. 4 e 5 del d.lgs. n. 216 del 29 dicembre 2017. In relazione all'ambito di operatività del disposto, ai sensi del novellato art. 266, comma 2, c.p.p. «[n]egli stessi casi [di cui al comma 1] è consentita l'intercettazione di comunicazioni tra presenti che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile» (art. 4, comma 1, lett. a), punto 1 d.lgs. n. 216 del 2017). Inoltre, il novellato comma 2-*bis* dell'art. 266 c.p.p. prevede che «[l]'intercettazione di comunicazioni tra presenti mediante l'inserimento di captatore informatico su un dispositivo elettronico portatile è sempre consentita nei procedimenti per i delitti di cui all'articolo 51, commi 3 bis e 3 quater» (art. 4, comma 1, lett. a, punto 2 d.lgs. n. 216 del 2017). In argomento, L. CAMALDO, *Le innovazioni previste dalla legge anticorruzione*

L'ulteriore dato di rilievo è fornito dall'avallo della legittimità del ricorso al *trojan* anche per le comunicazioni tra presenti. Qui, tuttavia, l'intrusione nel domicilio è consentita, se in quei luoghi si svolge l'attività criminosa, presupposto che non opera per i reati di cui agli artt. 51, commi 3-*bis* e 3-*quater*, c.p.p. e, come già accennato, per i delitti dei pubblici ufficiali (riferimento esteso anche agli incaricati di pubblico servizio⁴) contro la pubblica amministrazione puniti con la pena della reclusione non inferiore nel massimo a cinque anni determinata ai sensi dell'art. 4 c.p.p. (art. 266, comma 2-*bis*, c.p.p.).

Nei procedimenti relativi a questi ultimi reati, la riduzione della soglia di tutela si estende anche ad altri profili.

Invero, i delitti di criminalità organizzata e quelli contro la pubblica amministrazione vengono parificati in relazione ai presupposti ed alla durata dell'attività di intercettazione, in linea con quanto disposto dall'art. 13 del d.l. n. 152 del 1991, nonché rispetto al contenuto del decreto autorizzativo ed alla disciplina dell'urgenza.

Per vero, attraverso una modifica del comma 2-*bis* dell'art. 266 c.p.p.⁵, si è previsto che lo strumento può essere impiegato senza limiti spazio-temporali oltre che per i reati di cui all'art. 51, commi 3-*bis* e 3-*quater* c.p.p., per l'appunto, «per i delitti dei pubblici ufficiali o degli incaricati di pubblico servizio contro la pubblica amministrazione per i quali è prevista la pena della reclusione non inferiore nel massimo a cinque anni».

Rispetto alla formulazione previgente, il d.l. n. 161 del 2019 ha poi esteso, come detto, l'impiego del malware ai delitti commessi dagli incaricati di pubblico servizio, esclusi dalle precedenti formulazioni legislative⁶.

in tema di intercettazioni con captatore informatico, in *penale contemporaneo.it*, 24 settembre 2019; M. Torre, *Il captatore informatico dopo la legge spazzacorrotti*, in *Dir. pen. proc.*, 2019, 5, p. 648 ss.

⁴ Come noto, ex art. 357 c.p., sono considerati pubblici ufficiali «coloro che esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi»; sono, invece, incaricati di pubblico servizio ex art. 358 c.p., «coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata, dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale». Dunque, a titolo esemplificativo, è considerato pubblico ufficiale, l'insegnante, l'ufficiale giudiziario, l'ufficiale sanitario; è, invece, incaricato di pubblico servizio, una guardia giurata, un idraulico o un operaio del comune, il controllore dell'autobus o del treno.

⁵ Il decreto incide, conseguentemente, anche sull'art. 267 c.p.p., al fine di coordinarlo con la modifica del comma 2-*bis* dell'art. 266. Cfr. art. 2, comma 1, lett. f), punti 1 e 2 del decreto.

⁶ Di tal che, implementando le categorie dei soggetti per i quali il captatore informatico può trovare legittimamente utilizzo, il legislatore ne ha allargato indirettamente la portata anche ai reati ascrivibili in capo agli incaricati di pubblico servizio. In tale direzione, già la legge n. 3 del 9 gennaio 2019, c.d. «spazzacorrotti», aveva segnato un passaggio importante nella estensione della portata operativa del captatore informatico.

In questo scenario, anche se non sembra agevole cogliere la portata dell'intervento giurisprudenziale oggetto di commento – insinuandosi, esso, tra i diversi prodotti legislativi che hanno interessato il peculiare istituto captativo in disamina – si può, in maniera del tutto perspicua, enunciare il tema di fondo sul quale appuntare le riflessioni indotte dal caso concreto: il rapporto tra luogo di (presunta) perpetrazione delle condotte delittuose e modalità di effettuazione delle intercettazioni ambientali.

3. Le modalità intercettive quanto ai “luoghi” ed al “tempo”.

Qualsivoglia ragionamento che interessi il captatore informatico non può prescindere dalla esplorazione delle dinamiche di reciproca interferenza tra legislazione e prassi, muovendo dal presupposto, tanto ovvio quanto ineludibile, a mente del quale ci si trova al cospetto di un istituto di pura creazione giurisprudenziale.

Partendo da tale abbrivio, bisogna subito constatare come il legislatore si sia discostato dalla decisione “Scurato” quanto alla possibilità di effettuare intercettazioni «ubiquitarie»⁷ in un luogo di privata dimora, al di fuori della disciplina derogatoria contemplata per i delitti di criminalità organizzata di cui all'art. 13 del d.l. n. 152 del 1991.

Secondo i giudici di legittimità, infatti, non sarebbe possibile prevedere in anticipo i luoghi di privata dimora in cui il dispositivo elettronico si troverebbe e, di conseguenza, indicarli nel decreto autorizzativo del giudice per le indagini preliminari⁸. Specularmente, non sarebbe proficuo, per gli organi di polizia giudiziaria, seguire gli spostamenti del “bersaglio” e disattivare la captazione al momento dell'ingresso in un luogo di privata dimora⁹.

Il legislatore, dal suo canto, ha adottato una opzione diametralmente opposta a quella avallata per via nomofilattica, ritenendo ammissibile la captazione itinerante/domiciliare nel caso in cui vi sia il fondato motivo di ritenere che in un luogo di privata dimora si stia svolgendo attività criminosa¹⁰. L'art. 266, comma 2, secondo

⁷ Parla di intercettazioni ubiquitarie G. COROSANTI, *Le intercettazioni “ubiquitarie” e digitali tra garanzia di riservatezza, esigenze di sicurezza collettiva e di funzionalità del sistema delle prove digitali*, in *Diritto dell'Informazione e dell'Informatica*, 2016, 1, p. 88.

⁸ Per dirla con le parole della Cassazione: «all'atto di autorizzare una intercettazione da effettuarsi a mezzo di captatore informatico installato su di un apparecchio portatile, il giudice non può prevedere e predeterminare i luoghi di privata dimora nei quali il dispositivo elettronico [...] verrà introdotto, con conseguente impossibilità di effettuare un adeguato controllo circa l'effettivo rispetto della normativa che legittima, circoscrivendole, le intercettazioni domiciliari di tipo tradizionale» (Cass., Sez. Un., 1 luglio 2016, n. 26889, cit., p. 6).

⁹ Tale ragionamento può ricavarsi da un'argomentazione *ad absurdum* della stessa Corte di Cassazione: «peraltro, anche se fosse teoricamente 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 al momento dell'autorizzazione, che verrebbe disposta “al buio”» (Cass., sez. un., 1 luglio 2016, n. 26889, cit., p. 6).

¹⁰ Precisa T. ALESCI, *Le intrusioni inter praesentes*, in Bene (a cura di), *L'intercettazione di comunicazioni*, Bari, 2018, p. 77, che «il fondato motivo di ritenere non postula che detta attività debba essere stata effettivamente

periodo, c.p.p. non ha subito, di tal che, alcuna variazione, ponendosi in continuità con il precedente periodo che ammette le operazioni captative di che trattasi¹¹.

La possibilità di procedere alla avanguardistica intercettazione nei luoghi di cui all'art. 614 c.p., peraltro, è – implicitamente – corroborata dal disposto di cui al comma 2-bis dell'art. 266 c.p.p. nonché dal rafforzato onere motivazionale imposto al giudice per le indagini preliminari dall'art. 267, comma 1, ultimo periodo, c.p.p.: il giudice per le indagini preliminari deve indicare nel provvedimento autorizzativo «i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono».

I Giudici di legittimità al cospetto della problematica sollevata, di conseguenza, si sarebbero dovuti interrogare¹² sul livello di precisione richiesto al giudice per le indagini preliminari ai fini della indicazione, anche indiretta, dei “luoghi” e del “tempo”.

Il legislatore delegato era ben consapevole della difficoltà di prevedere, nel dettaglio, gli spostamenti di un dispositivo portatile e, di conseguenza, di indicare nel decreto autorizzativo i tempi ed i luoghi in cui attivare il microfono per la captazione audiofonica¹³; da tanto la necessità di fissare il margine argomentativo concesso al giudice per la statuizione autorizzativa, dal momento che una indicazione eccessivamente meticolosa avrebbe finito per rendere inutile lo strumento investigativo, mentre una indeterminatezza totale sarebbe sfociata nella illegittimità della tecnica captativa, poiché *ad explorandum*.

Il luogo, comunque, è uno dei due requisiti richiesti nel decreto giudiziale.

La novità della previsione, così, traccia una linea di cesura con quanto sancito dalle Sezioni unite Scurato, a mente delle quali l'indicazione logistica costituirebbe una mera modalità attuativa, funzionale a fornire indicazioni per l'esecuzione della intercettazione¹⁴. Viceversa, il legislatore ha ritenuto preferibile annoverare la

sussistente, dovendosi considerare sufficiente, sulla base del dato normativo [...], che dell'attività in questione possa, con giudizio *ex ante* ragionevolmente ritenersi la sussistenza dell'emanazione del provvedimento di autorizzazione all'effettuazione delle operazioni».

¹¹ Per semplicità espositiva si riporta il novellato art. 266, comma 2, c.p.p.: «negli stessi casi è consentita l'intercettazione di comunicazioni tra presenti, che può essere eseguita anche mediante l'inserimento di un captatore informatico su un dispositivo elettronico portatile. Tuttavia, qualora queste avvengano nei luoghi indicati dall'articolo 614 del codice penale, l'intercettazione è consentita solo se vi è fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa».

¹² Come fatto da C. GITTARDI, *Linee guida per l'applicazione del Decreto Legislativo 29.12.2017 n. 216 disposizioni in materia di intercettazioni di conversazioni o comunicazioni. Prime direttive alla Polizia Giudiziaria*, in *penalecontemporaneo.it*, 13 aprile 2018, p. 24 s.

¹³ Si legge, infatti, nella relazione di accompagnamento al d.lgs. n. 216 del 2017 che «la formula – secondo la quale nel decreto autorizzativo i luoghi e il tempo, in cui il dispositivo può essere attivato da remoto, possono essere “anche indirettamente determinati” – si spiega, dunque, nell'impossibilità di prevedere specificamente tutti gli spostamenti dell'apparecchio controllato; da qui la necessità logica di delimitare gli ambiti ai verosimili spostamenti del soggetto, in base alle emergenze investigative. A titolo esemplificativo, valga il riferimento a formule del tipo: “ovunque incontri il soggetto x”; “ogni volta che si rechi nel locale y ecc. ecc.». Anche la dottrina sul punto ha evidenziato «l'impossibilità di predeterminare con certezza gli spostamenti del supporto informatico sul quale insiste il *trojan horse*» (T. ALESCI, *Le intrusioni inter praesentes*, cit., p. 78).

¹⁴ «La tesi sostenuta nella sentenza n. 27100/15 in ordine alla necessità di individuare con precisione, a pena

indicazione del luogo – insieme a quella del tempo – tra i presupposti del provvedimento autorizzativo (art. 267, comma 1, c.p.p.), supportandola da una espressa comminatoria di inutilizzabilità del risultato intercettivo (art. 271, comma 1, c.p.p.)¹⁵; il tutto al fine di garantire un bilanciamento tra esigenze investigative ed istanze di *privacy*, assicurando un controllo postumo da parte dell'ignaro destinatario della attività captativa.

4. Le declinazioni della prassi.

Sul fronte delle prassi, la materiale difficoltà di determinare aprioristicamente il luogo di effettuazione della captazione sollecita, inevitabilmente, il rimando ad accadimenti della vita quotidiana, strettamente connessi alle peculiarità dei delitti per i quali si procede¹⁶.

A titolo esemplificativo¹⁷, si consideri il caso della lotta allo spaccio di sostanze psicotrope o stupefacenti.

Nel caso si giunga a conoscenza di un imminente incontro per la cessione di un ingente quantitativo di sostanza, ma non si sia a conoscenza dell'ubicazione del luogo dello scambio, il provvedimento autorizzativo della intercettazione itinerante potrebbe rimandare, indirettamente, al luogo dello scambio con una formula del tipo: “nel luogo in cui Tizio incontrerà Caio per cedergli la sostanza stupefacente”.

In tale prospettiva, si può immaginare che i giudici di merito faranno ricorso a formule generali ed ampie per saggiare la precisione della delimitazione spaziale; le quali, tuttavia, di per sé non possono assumere un significato precettivo se non calate nel peculiare orizzonte della fattispecie concreta¹⁸.

Simili problematiche paiono ancor più amplificate ove si accolga, come fanno alcuni¹⁹, una accezione estesa di domicilio, tale da abbracciare “anche” il ricorrente concetto di domicilio informatico²⁰. Così argomentando, il luogo di privata dimora nel

di inutilizzabilità, i “luoghi” nei quali le intercettazioni tra presenti devono essere espletate, si pone altresì in palese difformità rispetto alla consolidata giurisprudenza che ha sempre escluso la necessità di una tale indicazione ad eccezione dei luoghi di privata dimora, per i quali vale il disposto dell'art. 266 c.p.p., comma 2» (Cass., Sez. Un., 1 luglio 2016, n. 26889, cit., p. 8).

¹⁵ Nel previgente regime, dal momento che l'indicazione del tempo e del luogo non erano espressamente annoverati tra i presupposti del provvedimento, la sanzione dell'inutilizzabilità non era comminabile. Il rimando operato dall'art. 271 c.p.p. all'art. 267 c.p.p. deve oggi considerarsi esteso interamente a questo ultimo articolo.

¹⁶ D. PRETTI, *Prime riflessioni a margine della nuova disciplina sulle intercettazioni*, in *Dir. pen. cont.*, 2018, 1, p. 216.

¹⁷ D. PRETTI, *Prime riflessioni a margine*, cit., p. 221.

¹⁸ Si pensi che vi sono già nel panorama giurisprudenziale affermazioni di principio che assumono significato esclusivamente se calate nel panorama applicativo. A mero titolo esemplificativo si pensi alla definizione di atto abnorme quale «provvedimento caratterizzato dall'esercizio di un potere totalmente al di fuori del principio di tassatività delle impugnazioni di cui all'art. 568 cod. proc. pen.» (Cass., Sez. Un., 26 marzo 2009, n. 25957, in *C.E.D. Cass.*, n. 24359).

¹⁹ S. SIGNORATO, *Le indagini digitali. Profili strutturali di una metamorfosi investigativa*, Padova, 2018, p. 244 ss.

²⁰ Per un approfondimento della problematica, v., *ex multis*, R. KOSTORIS, *La costruzione dei diritti fondamentali, la Carta di Nizza e le prospettive di adesione dell'Unione alla Cedu*, in Kostoris, (a cura di), *Manuale di procedura*

quale viene effettuata l'intercettazione itinerante non si rinverrebbe nello spazio fisico nel quale è presente il dispositivo elettronico portatile infettato, bensì, nello smartphone stesso.

In altre parole, il captatore è la cimice, mentre il domicilio è lo smartphone, a condizione che quest'ultimo soddisfi «i requisiti dello *ius includendi se*; dello *ius includendi et excludendi alios* e della destinazione del luogo ad attività private tipiche della vita domestica o a spazio di attività lavorativa»²¹.

Corollario di tale ermeneusi: il fondato motivo di ritenere che “si stia svolgendo l'attività criminosa” andrebbe riferito al dispositivo elettronico portatile infetto e non già al luogo fisico in cui avviene la captazione, rimanendo così «del tutto residuale»²² l'ipotesi della intercettazione itinerante al di fuori di un luogo di cui all'art. 614 c.p.

L'approccio non sembra meritevole di condivisione se solo si esplora il valore semantico da attribuire alla nozione di luoghi “indirettamente determinati” ex art. 267, comma 1, c.p.p.

Prima facie potrebbe sostenersi che i luoghi sarebbero sempre determinati poiché non è dato comprendere come il dispositivo bersaglio possa essere indicato indirettamente. Tuttavia, il dispositivo bersaglio in uso ad un dato soggetto potrebbe non essere sempre lo stesso: l'utenza (*recte*: lo smartphone) oggetto di intercettazione potrebbe essere ceduta dal titolare ad un terzo; ovvero potrebbe accadere che il dispositivo *target* presenti dei malfunzionamenti o diventi inutilizzabile per i più vari motivi e, quindi, venga sostituito l'“organismo ospite”.

Ergo, la indicazione dei luoghi in modo indiretto potrebbe compendiarsi in formule generiche del tipo «il dispositivo mobile appartenente a Tizio», omettendosi qualsivoglia specificazione ulteriore, così consentendo l'intercettazione itinerante anche nel caso di successione nel tempo di dispositivi mobili.

Viepiù, un elemento di peculiare significanza sul fronte considerato è costituito dalla necessaria indicazione del tempo di attivazione del microfono già nel provvedimento autorizzativo della intercettazione itinerante, il quale si affianca – e non si sostituisce – alla durata delle disposte intercettazioni²³. Il dato, in tal modo, sancisce una netta cesura tra le captazioni tradizionali, le quali proseguono ininterrottamente per tutto l'arco temporale in cui sono autorizzate (normalmente 15 giorni ed eventuali successive proroghe), e quelle itineranti, i cui momenti temporali di attivazione necessitano di un apposito comando dell'autorità giudiziaria procedente²⁴, pur dovendo

penale europea, III ed., Milano, 2017, p. 51 ss.; S. SIGNORATO, *Le indagini digitali*, cit., p. 49 ss.; V. PAPA, *Espressione e diffusione del pensiero in Internet. Tutela dei diritti e progresso tecnologico*, Torino, 2009.

²¹ S. SIGNORATO, *Le indagini digitali*, cit., p. 246.

²² S. SIGNORATO, *Le indagini digitali*, cit., p. 246.

²³ L'indicazione delle coordinate temporali costituisce un elemento di novità significativa, dal momento che le «limitazioni spaziali costituivano già, a seconda dei casi, patrimonio della disciplina delle intercettazioni» (D. PRETTI, *Prime riflessioni a margine*, cit., p. 221).

²⁴ Non bisogna dimenticare che se il virus informatico agisse indisturbato per tutto l'arco della giornata, il dispositivo captato andrebbe incontro ad un repentino consumo di batteria e ad un ingente consumo di traffico dati, così mettendo a rischio la copertura investigativa. Sul punto, v. F. PIO, *Intercettazioni a mezzo captatore informatico: applicazioni pratiche e spunti di riflessione alla luce della recente decisione delle Sezioni Unite*,

rimanere confinate nel perimetro di durata massima della intercettazione²⁵.

Anche in questo caso il giudice per le indagini preliminari potrà ricorrere ad una indicazione «indirettamente determinata» del tempo in cui si potrà procedere alla intercettazione virale-ambientale, a condizione comunque che non autorizzi una captazione *ad explorandum*²⁶; ed anche in questo caso non sembrano potersi definire aprioristicamente, ed in linea teorico-astratta, criteri di orientamento avulsi da agganci a fattispecie concrete.

È comunque indubbio che la indicazione spaziale, unita a quella temporale, non deve determinare una dilatazione eccessiva dell'ambito applicativo dell'istituto²⁷, sebbene permanga la possibilità che elementi utili alle indagini possano disvelarsi in un momento in cui la captazione itinerante non è autorizzata.

Ovviamente, le considerazioni appena articolate non trovano operatività nei casi in cui si procede per uno dei delitti di cui all'art. 51, commi 3-bis e 3-quater, c.p.p., ai quali, come detto, si applica la menzionata disciplina derogatoria di cui all'art. 13 d.l. 152/1991²⁸.

in AA.VV., *Trojan horse: tecnologia, indagini e garanzie di libertà (profili di intelligence)*, in *parolaalladifesa.it*, 06 settembre 2016, p. 161.

²⁵ Esemplificando, se l'attività di intercettazione "tradizionale" è autorizzata dal giorno x al giorno y, è in questo lasso temporale (di 15 giorni) che il giudice deve indicare i tempi in cui il microfono potrà essere attivato, procedendo così all'intercettazione itinerante.

²⁶ Per esplicitare meglio l'assunto, si è fatto ricorso al seguente esempio: «si pensi al procedimento a carico di due sodali individuati quali autori di una rapina; ottenuta l'autorizzazione all'attivazione degli ascolti mediante *trojan horse* inoculato sul dispositivo telefonico portatile di uno dei due indagati in vista dell'incontro tra i due, in area campestre, per la spartizione del profitto del reato, potrà accadere che i due interlocutori si accordino, in quella sede, anche in vista di un ulteriore "colpo" da mettere a segno in seguito, dandosi appuntamento per un nuovo incontro finalizzato alla predisposizione delle specifiche modalità operative del nuovo reato da perpetrare. In tal caso, è possibile che l'autorizzazione abbia legittimato l'intercettazione in occasione del primo incontro limitando ad esso, e ad esso solo, la facoltà di attivazione del microfono, ragione per cui il decreto del pubblico ministero che ha disposto le operazioni avrà recepito la durata complessiva limitatamente a quell'incontro, con la conseguenza che sarà necessaria una nuova autorizzazione ed un nuovo decreto in vista dell'incontro successivo. Al contrario, è possibile ipotizzare anche che il giudice abbia autorizzato, indirettamente, la captazione in ragione di ogni incontro che si svolgerà in quel luogo (o in altri luoghi) in vista di tutte le possibili occasioni d'incontro tra i due sodali: in tal caso, non sarà necessaria una nuova autorizzazione e l'ascolto avrà luogo, con attivazione del microfono ad intermittenza, ad ogni occasione d'incontro, per tutta la durata fissata con il decreto del pubblico ministero, di cui si potrà comunque disporre la proroga ad opera del giudice» (D. PRETTI, *Prime riflessioni a margine*, cit., p. 221 ss.).

²⁷ V., ex multis, M. DI STEFANO, *Grande fratello sì, intercettazioni con lo smartphone ma solo per la criminalità organizzata*, in *Foro it.*, 2016, II, pp. 516 ss.

²⁸ Per tali delitti il compendio accusatorio *in fieri* non dovrà basarsi su «gravi indizi di reato» e su di una assoluta indispensabilità del mezzo di ricerca della prova ai fini della prosecuzione delle indagini (art. 267, comma 1, c.p.p.); ma i presupposti applicativi saranno soddisfatti da un quadro indiziario sufficiente («sufficienti indizi»), qualora l'intercettazione sia «necessaria ai fini dello svolgimento delle indagini» (art. 13 d.l. 152/1991). Quindi, sufficienti e non gravi indizi di reato, necessità e non assoluta indispensabilità ai fini dello svolgimento (non per la prosecuzione) delle indagini. Inoltre, il lasso temporale di utilizzo dello strumento captativo subisce una netta rimodulazione, laddove la legislazione speciale consente di ricorrere alle intercettazioni di comunicazioni o conversazioni telefoniche e di altre forme di telecomunicazione per un periodo iniziale di 40 giorni, con successive proroghe di 20, a fronte dei 15 giorni, con relative proroghe

5. Le cause di inutilizzabilità.

Gli itinerari ermeneutici tracciati consentono di apprezzare la indubbia significanza delle conclusioni rassegnate dalla Corte di legittimità: sebbene esperite in luogo pubblico o aperto al pubblico, le intercettazioni ambientali autorizzate rispetto ad uno specifico “luogo di privata dimora” all’interno del quale non si stia svolgendo attività delittuosa non sono utilizzabili.

Al contempo, tuttavia, non può omettersi di enfatizzare l’errore metodologico sul quale fonda la sentenza annotata, tale da svilirne la portata nella misura in cui la stessa trae scaturigine – esclusivamente – dai dettami della “sentenza Scurato”, oggetto di una ri-lettura non del tutto conferente.

In tale direzione, la ricostruzione delle linee normative ed esegetiche che hanno interessato lo sviluppo degli impieghi del captatore informatico dimostra come l’ancoraggio della sancita inutilizzabilità intercettiva ai contenuti della sentenza Scurato conduca a risultati opinabili, oltre che fuorvianti.

Ergo, è l’addentellato normativo ipostatizzato nelle richiamate previsioni di cui agli artt. 266 e 267 c.p.p. a corroborare la inappuntabilità dei risultati conseguiti sul fronte della inutilizzabilità dei risultati cognitivi acquisiti in maniera irrituale e, dunque, delle garanzie irrinunciabili e delle (fondamentali) prerogative individuali.

D’altro canto, la commendevolezza della soluzione prospettata, già sul fonte più propriamente metodologico, la si inferisce nel richiamo delle previsioni disciplinanti le “patologie” dei dati carpiti attraverso il cd. *trojan horse*.

È contemplato, infatti, che i risultati delle intercettazioni non possono essere utilizzati “fuori dei casi consentiti dalla legge” o se non siano state “osservate le disposizioni previste dagli art. 267 e 268 commi 1 e 3”, ossia le prescrizioni autorizzative ed operative (art. 271, comma 1, c.p.p.), nonché le disposizioni relative all’uso del captatore informatico (art. 271, comma 1-bis, c.p.p.).

Quanto ai requisiti di ammissibilità delle intercettazioni, l’art. 266 c.p.p., come visto, individua le categorie dei reati per i quali è consentito ricorrere allo specifico mezzo captativo, per titolo o secondo il livello di pena prevista.

Non sussistono, pertanto, particolari difficoltà per riscontrare quando l’intercettazione sia ammissibile, se non nel momento in cui intervenga la “modifica” del reato o si profilino fatti di reato nuovi o diversi rispetto alla contestazione utilizzata per la richiesta e la autorizzazione alla intercettazione.

Ad ogni modo, quanto alle ipotesi principali di inutilizzabilità *ex art. 271, comma 1, c.p.p.* dei risultati delle intercettazioni eseguite mediante captatore informatico appare chiaro che l’esecuzione “fuori dei casi consentiti dalla legge” rimanda agli artt. 266 c.p.p. e 266-bis c.p.p., nonché all’art. 13 del d.l. n. 152 del 1991, riferendosi, quindi, alla attività

di 15, prescritte dal codice di rito.

di captazione posta in essere per reati diversi da quelli per i quali le intercettazioni sono ammissibili.

Di conseguenza, nessun problema interpretativo discende dal richiamo, contenuto nell'art. 271 c.p.p., alla inutilizzabilità dei risultati delle intercettazioni "per inosservanza delle disposizioni di cui all'art. 267 c.p.p.", atteso che tale norma è richiamata nella sua integralità. Dunque, alla violazione delle disposizioni relative al cd. captatore informatico, introdotte dal d.lvo n. 216 del 2017, consegue la più grave sanzione della inutilizzabilità.

Insomma, saranno colpite da inutilizzabilità le intercettazioni tra presenti, mediante inserimento di captatore informatico su dispositivo elettronico portatile, nel caso in cui nel decreto autorizzativo manchi l'indicazione delle ragioni che rendono necessario il ricorso a tale modalità per lo svolgimento delle indagini.

Invece, per i reati diversi da quelli di cui all'art. 51, commi 3-bis e 3-quater, c.p.p. e dai reati dei pubblici ufficiali e degli incaricati di pubblico servizio contro la pubblica amministrazione puniti con pena non inferiore a 5 anni di reclusione, saranno sanzionati con la inutilizzabilità i risultati di quelle intercettazioni tra presenti, mediante inserimento di captatore informatico su dispositivo elettronico portatile, allorché nei decreti autorizzativi manchi l'indicazione dei luoghi e del tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono.

Tutto questo determina ovvie implicazioni di carattere pratico.

L'unica condizione legittimante l'impiego del captatore, qualora l'intercettazione avvenga in luoghi domiciliari e qualora si proceda per reati "non" di criminalità organizzata, è che sia dimostrata la attualità dello svolgimento dell'attività criminosa in tali luoghi.

Orbene, posto che la precipua preclusione a fondamento della limitazione imposta dalle Sezioni unite "Scurato" discende da un parametro di natura squisitamente tecnica in ordine alla certezza del luogo ove il monitoraggio dovrebbe avvenire, allorché il legislatore adotta una soluzione differente, indirettamente smentendo tale asserto, dimostra che con gli accorgimenti del caso è possibile conoscere, con certezza, i luoghi ove i soggetti monitorati si trovino durante le comunicazioni.

L'approccio autorizza, quindi, una lettura evolutiva della pronuncia della Suprema corte.

Nondimeno, è stato lo stesso legislatore, con il d.lgs n. 216 del 2018, art. 4 comma 1) lett. b) n. 1, ad aver circoscritto l'utilizzabilità del captatore informatico, disponendo che "se si procede per delitti diversi da quelli di cui all'articolo 51, commi 3-bis e 3-quater, [indica] i luoghi e il tempo, anche indirettamente determinati, in relazione ai quali è consentita l'attivazione del microfono".

In altre parole, consapevole della particolare insidiosità del predetto strumento per la riservatezza delle informazioni, al fine di evitare che esso possa essere adoperato per monitorare in modo indiscriminato i soggetti interessati ovunque e con chiunque si trovino, il legislatore ne ha sancito il ricorso limitatamente alle ipotesi in cui, alla luce delle circostanze concrete, risulti impossibile adoperare i tradizionali strumenti.

Anche per tale via risulta pienamente condivisibile lo spirito che ha animato la sentenza in commento, non potendosi avallare l'uso generalizzato del captatore

informatico per il sol fatto che ci si trovi al cospetto di luoghi pubblici o aperti al pubblico – al di là di tempi e dei luoghi (non)specificamente indicati –.

Non a caso, dalla lettura dei lavori preparatori della riforma Orlando (l. 23 giugno 2017, n. 103), le indicazioni palesanti una parziale rilettura del quadro delineato dalla giurisprudenza di legittimità²⁹ sono assai più precise di quanto statuito in tema di intercettazioni “tradizionali” ed, in questa sede, non possono che essere analiticamente richiamate.

a) L’attivazione del microfono potrà avvenire solo a seguito di un apposito comando inviato da remoto e non dal mero inserimento del captatore informativo, e ciò sempre nel rispetto dei limiti stabiliti da un decreto autorizzativo emanato da un giudice.

b) La registrazione audio dovrà essere avviata dalla polizia giudiziaria o dal personale incaricato su indicazione della polizia operante, la quale sarà tenuta ad indicare necessariamente 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 c.p.p.

c) 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. e, fuori da tali casi, potrà essere disposta nei luoghi di cui all’art. 614 c.p. soltanto se negli stessi si stia svolgendo l’attività criminosa. In ogni caso, il necessario decreto autorizzativo del giudice dovrà indicare le ragioni per cui tale modalità di intercettazione particolarmente invasiva sia necessaria per lo svolgimento delle investigazioni.

d) Le intercettazioni così ottenute potranno essere utilizzate ai fini probatori soltanto per i reati oggetto del provvedimento autorizzativo e potranno essere impiegate in procedimenti diversi a condizione che siano indispensabili per l’accertamento di uno dei delitti di cui all’articolo 380 c.p.p.

Anche tali considerazioni consentono di apprezzare l’arresto giurisprudenziale in disamina, avuto specifico riguardo per prodotti legislativi promulgati a far data dal 2017.

6. Riflessioni conclusive.

La posizione espressa dal Supremo collegio assume rilievo ancor più pregnante se si considera che il primo settembre è entrata in vigore la riforma delle intercettazioni e, soprattutto, la biasimata disciplina che consente la inedita “pesca a strascico” mediante captatore informatico.

Dunque, le affermazioni di principio – di assoluta garanzia – dei giudici di legittimità paiono ancor più significative nella misura in cui con esse si mira a porre un argine allo strapotere investigativo del captatore informatico.

Sono ormai note le problematiche implicate da uno strumento tanto invasivo: un virus che riesce ad entrare, con inganno, nell’apparecchio che si vuole intercettare, non

²⁹ Cfr. C. PARODI, *La riforma “Orlando”: la delega in tema di “captatori informatici”*, Bologna, 2017, p. 38 ss.

per distruggerlo né tanto meno per danneggiarlo, ma per carpire qualsiasi dato ivi possa trovarvisi.

Un meccanismo, per vero, concepito per istallarsi in modo occulto sui congegni elettronici che si vuole monitorare ed agendo senza far rilevare all'utente la propria presenza.

L'ufficiale di polizia giudiziaria che opera tale controllo, in particolare, può decifrare tutto ciò che viene digitato sulla tastiera; visualizzare quel che appare sullo schermo; monitorare la navigazione in internet; perquisire i *files* contenuti nell'hard disk o salvati in cloud; accedere alle applicazioni di posta elettronica e di messaggia; visualizzare gli sms inviati e ricevuti ed intercettare quelli in entrata e uscita; carpire le conversazioni telefoniche; attivare il microfono ed effettuare intercettazioni ambientali nel raggio di una decina di metri dall'apparecchio; attivare la videocamera e riprendere quanto viene inquadrato.

Insomma, il captatore informatico è in grado di penetrare nell'intimità di una persona in una misura finora sconosciuta, tanto profonda quanto pervasiva³⁰.

Non a caso, si è detto – forse in un pizzico di esagerazione – che l'intrusione informatica rasenta il controllo psichico.

Senza dubbio, il monitoraggio e la captazione in tempo reale da remoto di tutta la sfera individuale fa sembrare l'intercettazione su un'utenza telefonica o la videoripresa in una certa abitazione strumenti vecchi e polverosi.

Ecco perché l'intrusione informatica sollecita – sempre e comunque – profonde riflessioni; ecco perché vanno salutate con favore certe prese di posizione funzionali ad invaginare le immani – e forse non completamente esplorate – potenzialità investigative del captatore informatico entro ambiti di stretta legalità, che forniscono lo spunto anche per riflessioni *de iure condendo*.

A tal uopo, il reale aspetto problematico trascurato dalle novelle legislative innanzi richiamate è rappresentato dalla più volte rammentata natura “mobile” e dunque “itinerante” dello strumento intercettizio, che inevitabilmente potrebbe interferire con i beni primari di terzi estranei all'attività di indagine. In proposito, se è vero che la possibilità di intercettazione mediante captatore in ambiente domiciliare, pur in assenza del *fumus perdurantis delicti*, è stata limitata ai reati di cui all'articolo 51, commi 3-bis e 3-quater, c.p.p. è altrettanto vero che il nuovo strumento captativo si sposta con chi detiene il dispositivo “infettato”. Ragione per la quale, nelle indagini relative a quei reati, in assenza di un onere di indicazione preventiva dei luoghi (*ex art. 267, comma 1*), l'intercettazione è destinata ad operare in una pluralità di domicili, cioè presso i luoghi di privata dimora di chiunque venga in contatto con il soggetto intercettato, con inevitabile lesione della libertà *ex art. 14 Cost. dei terzi*. Né l'onere di motivazione del decreto che autorizza l'intercettazione mediante captatore, rafforzato dalla necessaria indicazione delle “ragioni che rendono necessaria tale modalità per lo svolgimento delle indagini” (*art. 267, comma 1, secondo periodo*), sembra rappresentare un argine sufficiente per i possibili abusi dello strumento.

³⁰ G. PICA, *Diritto Penale delle tecnologie informatiche*, Torino, 1999, p. 66.

Peraltro, sembra da ricondurre ad imperfezione tecnica il riferimento allo svolgimento delle indagini anziché alla loro prosecuzione. Il coordinamento tra primo e secondo periodo del comma 1 dell'art. 267 c.p.p. vale a "neutralizzare" sul piano interpretativo il rischio che si possa ritenere attivabile il captatore informatico anche "ai fini" dello svolgimento e non solo "della prosecuzione" delle indagini. Inoltre, non può non osservarsi che la previsione di uno sforzo motivazionale ulteriore da parte del giudice lascia intendere come il legislatore – al di là dell'equiparazione "di principio" tra intercettazioni tra presenti tradizionali ed intercettazioni mediante agente intrusore – ne abbia valutato la differenza, avendo appunto imposto uno specifico onere motivazionale o, per dirla altrimenti, un ulteriore requisito applicativo per le seconde intendendo, di conseguenza, responsabilizzare gli operatori del diritto ad adottare, *cum grano salis*, tale strumento di ascolto, ricorrendovi non solo ove non sia diversamente surrogabile, ma soprattutto introducendo — per l'appunto — un onere di motivazione aggiuntiva da inserire nel decreto autorizzativo.

In tale prospettiva, l'approccio è stato francamente troppo timido. Sarebbe stato quanto mai opportuno, ad esempio, contemplare stringenti vincoli di allegazione da parte del pubblico ministero nella richiesta, con corrispondenti obblighi di motivazione da parte del giudice nel decreto autorizzativo. Ciò in relazione a due specifici aspetti, del tutto trascurati dalla disciplina in disamina. In primo luogo, con riferimento alla necessaria relazione tra la persona intercettata ed il fatto-reato su cui si indaga, magari rivedendo il presupposto dei gravi (o sufficienti) indizi di reato e sostituendolo con una connessione soggettiva all'indagine (indizi di colpevolezza).

Sulla rilevanza della sussistenza di un collegamento diretto tra la persona intercettata ed indagine in corso, si era, tra l'altro, opportunamente soffermata proprio la Suprema Corte nella vicenda Romeo³¹, ove si era precisato che il giudice, nel provvedimento autorizzativo, deve necessariamente dar conto delle ragioni che impongono l'intercettazione di una determinata utenza telefonica che fa capo ad una specifica persona, "indicando...il collegamento tra l'indagine in corso e la medesima, affinché possa esserne verificata, alla luce del complessivo contenuto informativo e argomentativo del provvedimento, l'adeguatezza rispetto alla funzione di garanzia prescritta dall'articolo 15, comma 2, della Costituzione".

In secondo luogo, in relazione alla affidabilità della qualificazione giuridica del fatto, che avrebbe dovuto essere ancorata a sufficienti, sicuri ed obiettivi elementi indiziari, così come proposto in un fondamentale passaggio della motivazione della sentenza "Scurato".

E però, nessuno di questi spunti è stato recepito nei progetti di riforma analizzati.

Altrettanto poco condivisibile, la modifica dell'art. 271 c.p.p. in tema di inutilizzabilità.

Con l'inserimento del comma 1-*bis*, il legislatore ha specificato che sono "in ogni caso" inutilizzabili "i dati acquisiti nel corso delle operazioni preliminari all'inserimento

³¹ Cass., Sez. VI, 13 giugno 2017, n. 36874, in *C.E.D. Cass.*, n. 254478.

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”.

La nuova ipotesi di inutilizzabilità – che all’apparenza sembra perseguire l’esigenza di tutela delle garanzie della persona sottoposta a procedimento penale e, più in generale, dei diritti fondamentali dell’individuo – appare piuttosto come un rozzo tentativo di celare inconfessabili verità. Anzitutto, in punto di tecnica normativa, la disposizione non pare di grande utilità, stante il generale divieto, sancito dal primo comma dell’art. 271 c.p.p., di utilizzo dei risultati delle intercettazioni eseguite fuori dei casi consentiti dalla legge. Dunque, non trattasi di una disposizione che eleva la soglia delle garanzie individuali – come invece sarebbe stato necessario – in considerazione della particolare invasività dello strumento considerato.

A ben vedere, comunque, non è nemmeno una disposizione di armonizzazione interna della disciplina esistente rispetto al *novum* normativo, superflua ma innocua. Una semplice previsione di raccordo avrebbe, invero, richiesto differente tecnica di “redazione” (“le disposizioni di cui all’articolo...si applicano anche ai risultati delle intercettazioni eseguite mediante captatore...”).

L’aspetto più allarmante della vicenda, comunque, è altro. Il riferimento ai “dati” acquisiti nel corso delle operazioni preliminari ed al di fuori dei limiti del provvedimento autorizzativo se da un lato rappresenta una scontata conferma delle potenzialità intrusive del captatore, dall’altro, desta estrema preoccupazione, essendo ben più ampio della locuzione “risultati delle intercettazioni” utilizzata nel primo comma. I dati che possono essere acquisiti inoculando un *malware* sono – come si è visto – potenzialmente infiniti: suoni, immagini, documenti, conversazioni mediante applicativi di *instant messaging*, siti web visitati, tasti digitati, *files*, e-mail, rubriche telefoniche, appunti, agende, geo-localizzazione ed altro ancora. E la sanzione dell’inutilizzabilità postuma – cioè soltanto dopo che ne sia avvenuta l’acquisizione – è del tutto inefficace, essendo evidente che la lesione dei diritti attinti dalla illegittima apprensione si realizza nel momento stesso in cui questa si consuma e non semplicemente inibendone l’utilizzo processuale.

A cagione di tanto, il legislatore avrebbe dovuto prevedere – in un’ottica di doverosa tutela dei beni primari attinti dallo strumento – il divieto assoluto di acquisizione di qualunque dato al di fuori delle intercettazioni autorizzate, cui avrebbe dovuto corrispondere l’obbligo di immediata distruzione in caso di violazione della prescrizione, con un corredo sanzionatorio di matrice penale e disciplinare nei casi di abuso.