DIRITTO PENALE CONTEMPORANEO

L'USO DI CAPTATORI INFORMATICI (*TROJANS*) NELLE INTERCETTAZIONI "FRA PRESENTI"

Commento a Cass. pen., Sez. un., sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889, Pres. Canzio, Rel. Romis, Imp. Scurato

di Giulia Lasagni

Abstract. *Con questa attesa pronuncia, le Sezioni unite riconoscono la legittimità, per i delitti di criminalità organizzata, delle intercettazioni "fra presenti" anche senza la previa indicazione dei luoghi dove devono svolgersi.*
In particolare, la Cassazione ammette ufficialmente la possibilità di utilizzare a fini di surveillance *captatori informatici del tipo* Trojan*, capaci di attivare a distanza dispositivi che tipicamente seguono i soggetti intercettati in tutti i loro spostamenti (*smartphone, tablet, computer, Apple watch*...).*
Il presente contributo ricostruisce il percorso argomentativo delle Sezioni unite, collocandolo nell'attuale contesto storico-giurisprudenziale, in Italia e nell'Unione europea, e mettendo in evidenza i profili garantistici che devono essere rafforzati per far fronte all'ingresso di queste tecnologie nel campo delle indagini penali.

1. Introduzione.

L'ingresso della tecnologia digitale nel processo penale rappresenta ormai un dato di fatto. Negli ultimi anni e già in numerose occasioni, la giurisprudenza di merito e quella di legittimità si sono espresse sulle indagini effettuate grazie ad alcune tipologie

di c.d. "captatori informatici", quali navigatori satellitari[1] o programmi di clonazione degli *hard disk* (ad esempio "*ghost*")[2].

Rispetto a tali mezzi, tuttavia, l'uso di *software* informatici di controllo da remoto, come i *Trojan*, presenta indubbie peculiarità, come riconosciuto dalle Sezioni unite nella sentenza in commento.

In primo luogo, a differenza di altri strumenti intrusivi, questi *software* possono essere installati ed attivati sul dispositivo da intercettare in modo occulto ed a distanza (ad esempio tramite una e-mail, un'applicazione di aggiornamento, un sms).

In secondo luogo, questi captatori permettono una gamma molto ampia di operazioni intrusive, che comprendono: l'accesso (con facoltà di copia) ai dati memorizzati nel dispositivo, la registrazione del traffico dati in arrivo o in partenza (incluso quanto digitato sulla tastiera), la registrazione delle telefonate e delle videochiamate e, soprattutto, l'attivazione delle funzioni microfono e/o telecamera indipendentemente dalla volontà dell'utente.

In questo ultimo caso, il dispositivo può quindi essere utilizzato come strumento per registrare tutto ciò che avviene entro il proprio raggio di azione, sfruttando l'abitudine, ormai comune, di portare sempre con sé certi tipi di apparecchi digitali – quali *tablet* o *smartphone*, ma anche e sempre più orologi o occhiali che includono sistemi operativi c.d. *smart*, come gli *Apple watch* o i *Google glass*. Proprio queste attività di *surveillance*, non più limitate ad uno specifico luogo fisico, costituiscono l'oggetto della pronuncia in esame, con la quale le Sezioni unite ne riconoscono la legittimità alla luce dell'ordinamento interno.

Il fatto che solo recentemente[3] la Corte di cassazione abbia preso posizione per la prima volta in merito all'uso di *software* in grado di captare sia flussi di dati che di comunicazioni, tuttavia, non deve trarre in inganno circa l'entità dell'impiego di questi strumenti nella prassi investigativa. Dubbi sulla disciplina applicabile a questo tipo di intercettazioni erano già stati sollevati in diverse pronunce dei giudici di merito (fra cui

---

[1] Cass., Sez. I, 7 gennaio 2010, dep. 9 marzo 2010, n. 9416, Pres. Fazzioli, Rel. Cassano, Imp. Congia e a., C.E.D. 246774.

[2] Cass., Sez. V, sent. 14 ottobre 2009, dep. 29 aprile 2010, n. 16556, Pres. Calabrese, Rel. Pizzuti, Imp. Virruso e a., C.E.D. 246954, già commentata da ATERNO, *Le investigazioni informatiche e l'acquisizione della prova digitale, in Giur. merito*, 2013, p. 955 ss. e da TORRE, *Il* virus *di Stato*, cit., p. 1164.

[3] Nei casi precedenti in cui la Cassazione si era espressa in merito all'uso di captatori informatici, infatti, le potenzialità degli strumenti utilizzati a scopo di sorveglianza (ad esempio c.d. *ghost*) erano limitate prevalentemente alla captazione di dati, cfr. Cass., sent. 14 ottobre 2009, n. 16556, Virruso, cit.; Cass., Sez. IV, 17 aprile 2012, dep. 24 maggio 2012, n. 19618, Pres. Sirena, Rel. Massafra (meglio conosciuto come caso *Ryanair*) in *Cass. pen*., 2013, p. 1523 ss. con nota di BONO, *Il divieto di indagini* ad explorandum *include i mezzi informatici di ricerca della prova*, commentato anche da CORRIAS, *Perquisizione e sequestro informatici: divieto di* inquisitio generalis, in *Dir. informaz*., 2012, p. 1146.
Per una accurata ricostruzione del tema delle perquisizioni online nel nostro ordinamento si veda anche IOVENE, *Le c.d. perquisizioni online tra nuovi diritti fondamentali ed esigenze di accertamento penale*, in *Dir. Pen. Cont. – Riv. Trim.*, 3-4/2014, p. 329.

i noti provvedimenti emanati dal Tribunale di Palermo[4], o dal Tribunale di Napoli nel famigerato caso *Bisignani* concernente l'associazione di stampo massonico P4[5]), a testimonianza di un'operatività ormai diffusa di questi captatori informatici "polivalenti" nel nostro ordinamento.

2. Il contesto.

La sentenza prende le mosse dal ricorso per Cassazione contro l'ordinanza di conferma della misura di custodia cautelare emessa dal Tribunale del riesame di Palermo in data 8 gennaio 2016. L'indagato, accusato (anche) di partecipazione all'associazione mafiosa "Cosa Nostra", era stato sottoposto alla misura sulla base degli indizi emersi da una serie di intercettazioni "ambientali" svolte tramite *software* del tipo *Trojan* e dalle dichiarazioni accusatorie rilasciate da due collaboratori di giustizia.

L'ordinanza veniva impugnata per diversi motivi, fra cui l'asserita inutilizzabilità delle intercettazioni per violazione dell'art. 266 comma 2 c.p.p. sotto due profili.

Innanzitutto, la difesa riteneva che non fosse stato rispettato il divieto di eseguire intercettazioni all'interno di abitazioni private, giacché la captazione sarebbe stata autorizzata senza che in tali luoghi si stessero svolgendo attività criminose: di qui la conseguente violazione della riserva di legge prevista dall'art. 14 Cost. Le intercettazioni, infatti, così come risultanti dal decreto di autorizzazione, erano state svolte anche all'interno dell'abitazione della moglie del reggente del mandamento locale, ora detenuto, con cui l'indagato era spesso in contatto, operando sia come intermediario fra la signora ed il nuovo reggente in carica, sia come gestore delle estorsioni e del traffico di stupefacenti sul territorio.

In seconda battuta si contestava che, in ogni caso, la captazione fosse stata disposta senza indicare precisamente dove avrebbe dovuto essere effettuata. Ciò avrebbe comportato la violazione non solo della norma codicistica, ma anche delle garanzie poste a tutela dei diritti fondamentali previsti dagli art. 15 Cost. e 8 CEDU. In particolare, la difesa lamentava una insufficiente descrizione dei luoghi nel decreto di autorizzazione, che si limitava ad indicare genericamente lo svolgimento dell'attività di captazione ove fosse «ubicato in quel momento l'apparecchio portatile».

L'interpretazione proposta dal difensore, secondo cui la precisazione del luogo costituisce un requisito di legittimità dell'intercettazione, era ripresa da una sentenza

[4] Trib. Palermo, Sez. riesame, ord. 11 gennaio 2016, Pres. est. Gamberini, pubblicata in *questa Rivista*, 24 marzo 2016, con commento di LORENZETTO, *Il perimetro delle intercettazioni ambientali eseguite mediante ''captatore informatico''*.

[5] Proc. pen. n. 39306/2007 R.G.N.R., mod. 21, già commentato da TESTAGUZZA, *I sistemi di controllo remoto: fra normativa e prassi*, in *Dir. pen. e proc.*, 2014, p. 759 e ss., e da TORRE, *Il* virus *di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali*, in *Dir. pen. e proc.*, 2015, p. 1167.

della stessa Cassazione del 2015 (n. 27100, imputato Musumeci)[6]. In tale pronuncia, la Sezione VI, esprimendosi su un caso analogo a quello di specie, aveva infatti affermato che la formulazione dell'art. 266, comma 2 c.p.p. implicherebbe l'obbligo di specificare, nel decreto di autorizzazione, il luogo in cui le captazioni devono svolgersi. A sostegno di questo orientamento, in quella sede i giudici di legittimità avevano ritenuto tale lettura l'unica compatibile con il dettato dell'art. 15 Cost. L'uso di uno strumento di *surveillance* capace di seguire il soggetto in qualunque luogo esso si trovi risulterebbe, quindi, sempre illegittimo per violazione della libertà e della segretezza delle comunicazioni. Detta interpretazione troverebbe conferma, sempre secondo la medesima sentenza, anche in quella giurisprudenza che ammette la variazione del luogo in cui si devono svolgere le intercettazioni «solo se rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata»[7].

2.1. L'ordinanza di rimessione alle Sezioni unite.

Sul ricorso dell'indagato si esprimeva di nuovo la Sezione VI che stavolta, discostandosi dall'interpretazione del 2015, decideva di rimettere la questione alle Sezioni unite[8] tenuto conto della delicatezza della materia, della diffusione e relativa semplicità di applicazione di captatori informatici, nonché degli interessi costituzionali in gioco, «anche al fine di evitare potenziali contrasti giurisprudenziali in merito[9].

In particolare i giudici di legittimità, pur ribadendo l'incompatibilità tecnica fra il ricorso al *software Trojan* e la possibilità di predeterminare i luoghi di captazione, non ritenevano sussistente alcuna base legale per imporre quest'ultimo requisito ai fini della legittimità del mezzo di ricerca della prova. La Sezione VI rilevava che tale obbligo non

---

[6] Cass., Sez. VI pen., sent. 26 maggio 2015, dep. 26 giugno 2015, n. 27100, Pres. Milo, Rel. Di Salvo, Imp. Musumeci, pubblicata anche in *questa Rivista*.

[7] In tal senso: Cass., Sez. VI, sent. 11 dicembre 2007, dep. 11 aprile 2008, n. 15369, Pres. Lattanzi, Rel. Fidelbo, Imp. Sitzia C.E.D. 239634; Sez. V, sent. 6 ottobre 2011, dep. 15 febbraio 2012, n. 5956, Pres. Marasca, Rel. Oldi, Imp. Ciancitto, C.E.D. 252137; Sez. II, sent. 15 dicembre 2010, dep. 4 febbraio 2011, n. 4178, Pres. Esposito, Rel. Rago, Imp. Fontana, C.E.D. 249207; Sez. II, sent. 8 aprile 2014, n. 17894, dep. 29 aprile 2014, Pres. Esposito, Rel. Rago, Imp. Alvaro e a., in *Cass. pen.*, 2015, p. 1397, con nota di PAOLONI, *Il ruolo della borghesia mafiosa nel delitto di concorso esterno in associazione di stampo mafioso: un esempio della perdurante attualità delle Sezioni unite "Mannino"*.

[8] Cass., Sez. VI, ord. 10 marzo 2016, dep. 6 aprile 2016, n. 13884, Pres. Carcano, Rel. Fidelbo, Imp. Scurato, pubblicata in *questa Rivista*.

[9] Cfr. ord. 13884/2016, p. 10: «In particolare, le questioni che possono derivare da un possibile contrasto giurisprudenziale possono essere cosi sintetizzate:
- se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione;
- se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora a/ di fuori dei presupposti indicati dall'art. 266, *comma 2, cod. proc. pen.;*
- se *possa comunque prescindersi da tale indicazione net caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata».*

fosse desumibile né dalla legge, né da altra giurisprudenza a livello nazionale o sovranazionale, con riferimento specifico alla Corte europea dei diritti dell'uomo[10]. La rilevanza dell'indicazione del luogo, infatti, emergerebbe solo nel caso in cui l'operazione di captazione debba avvenire in abitazioni o luoghi privati; tale restrizione, tuttavia, non opera in riferimento ai procedimenti per i "delitti di criminalità organizzata" per cui vige la disciplina derogatoria speciale prevista dall'art. 13 d.l. 13 maggio 1991, n. 152 (convertito nella legge 12 luglio 1991, n. 203). In ogni caso, si sosteneva nella medesima ordinanza, la mancata descrizione dell'ambiente specifico dove l'intercettazione deve svolgersi potrebbe comunque essere compensata da un controllo postumo sull'utilizzabilità del materiale raccolto da effettuarsi, ad esempio, durante l'udienza "stralcio" di cui all'art. 268 comma 6 c.p.p. o, in caso di procedimento *de libertate*, conferendo facoltà al difensore di ottenere la trasposizione su nastro magnetico delle intercettazioni svolte.

3. Le motivazioni della Corte.

Con la sentenza in esame le Sezioni unite rigettano il ricorso dell'indagato, confermando la corrente interpretativa inaugurata dalla Sezione rimettente a discapito di quanto affermato nel 2015 in *Musumeci*. Così facendo i giudici di legittimità, intervenendo sul contrasto interpretativo fra due diversi orientamenti espressi dalla stessa Sezione VI a poco meno di un anno di distanza fra loro, contemporaneamente ricostruiscono la disciplina dei presupposti per le intercettazioni "fra presenti" e avallano ufficialmente l'ingresso, nel nostro ordinamento, dei captatori informatici "polivalenti" come strumenti di indagine penale.

3.1. La definizione di "captatore informatico" e le proposte legislative in materia.

Opportunamente, la Corte inizia la disamina del problema definendo le caratteristiche tecniche giuridicamente rilevanti dello strumento di captazione *Trojan* e sottolineandone le ampie potenzialità nell'effettuare intercettazioni «caratterizzate da modalità sostanzialmente di natura ambientale». Le Sezioni unite, inoltre, evidenziano chiaramente come la soluzione della questione[11] imponga un difficile bilanciamento fra le esigenze investigative di repressione di fenomeni criminosi, certamente avvantaggiate grazie all'uso della tecnologia informatica, e le garanzie dei diritti individuali, posto che

[10] In questa sede, inoltre, contrariamente a quanto sostenuto in *Musumeci*, la giurisprudenza in tema di variazione dei luoghi veniva considerata un elemento utile per sostenere la non rilevanza dell'indicazione di un luogo specifico nel decreto di autorizzazione.

[11] Riassunta nell'unico quesito espresso a p. 7 della sentenza: «*Se – anche nei luoghi di privata dimora ex art. 614 cod. pen., pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa – sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un 'captatore informatica' in dispositivi elettronici portatili (ad es., personal computer, tablet, smartphone, ecc.)*».

dall'applicazione di tali tecniche di controllo possono derivare lesioni gravi alle prerogative della persona.

In via preliminare, la Corte illustra quindi i diversi tentativi intrapresi sino ad oggi per creare una disciplina legislativa delle intercettazioni, comprensiva anche dell'uso di captatori informatici. Viene preso in considerazione il d.l. 18 febbraio 2015, n. 7, con cui nell'ambito del contrasto al terrorismo si era proposto di inserire nell'art. 266-*bis* c.p.p. la possibilità di eseguire le intercettazioni informatiche anche «attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico». La proposta di modifica, che avrebbe esteso la propria applicazione a tutti i reati inclusi nella disciplina comune delle intercettazioni, aveva suscitato preoccupazione presso l'opinione pubblica e, alla fine, non era stata approvata in sede di conversione, neppure dopo un emendamento che ne restringeva effettivamente l'applicazione solo ai delitti commessi con finalità di terrorismo[12]. Tentativi simili venivano presentati anche nelle proposte di legge C. 3470 del 2 dicembre 2015[13] e C. 3762 del 20 aprile 2016[14], ad oggi ancora senza esito.

3.2. Intercettazioni "ambientali" e intercettazioni "fra presenti": la rilevanza del "luogo" nel decreto di autorizzazione.

Svolte tali premesse, le Sezioni unite dispiegano le proprie argomentazioni a partire dall'unico punto condiviso sia dall'ordinanza di rimessione sia dalla sentenza *Musumeci*, ovvero l'inquadramento delle attività di indagine poste in essere su comunicazioni informatiche attraverso l'uso di *software* nella categoria delle intercettazioni «c.d. "ambientali"» di cui all'art. 266 comma 2 c.p.p.: è proprio sulla definizione dei relativi limiti applicativi, infatti, che i giudici di legittimità elaborano la soluzione ermeneutica più innovativa e rilevante della pronuncia in esame.

Innanzitutto, la Cassazione chiarisce come il termine "intercettazione ambientale" non abbia riscontro in nessun testo normativo, nemmeno nello stesso art. 266 comma 2 c.p.p., dove si parla invece di intercettazione di "comunicazioni fra presenti". Il riferimento ad un preciso contesto topografico è previsto solo nella seconda parte dell'art. 266 comma 2 c.p.p., quando però si prendono in considerazione i luoghi indicati dall'art. 614 c.p. ovvero, principalmente, la privata dimora.

La necessità di indicare con precisione e a pena di inutilizzabilità i luoghi nei quali le intercettazioni tra presenti devono essere effettuate non trova riscontro nemmeno nella giurisprudenza di legittimità che – fino alla sentenza del 2015 – non

---

[12] Come riscontrabile nella legge di conversione 17 aprile 2015, n. 43. In tal senso si veda, ad esempio, *Il disegno di legge antiterrorismo contiene una norma anticostituzionale*, in *Il Post*, 26 marzo 2015.

[13] Proposta di legge d'iniziativa della deputata Greco, *Modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche*.

[14] Proposta di legge d'iniziativa dei deputati Quintarelli e Catalano, *Modifiche al codice di procedura penale e alle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, in materia di investigazioni e sequestri relativi a dati e comunicazioni contenuti in sistemi informatici o telematici*.

aveva mai richiesto tale elemento quando le operazioni captative dovessero svolgersi in ambienti diversi dalla privata dimora[15]. L'indicazione preventiva, infatti, è funzionale alla verifica del presupposto del «fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa» e, quindi, al rispetto della riserva di legge prescritta dall'art. 14 Cost. Pertanto, concludono le Sezioni unite, contrariamente a quanto sostenuto in *Musumeci*, ritenere l'indicazione del luogo un requisito sempre necessario per la legittimità delle intercettazioni è un'affermazione priva di effettiva base legale nell'ordinamento interno.

Parimenti, e di nuovo all'opposto di quanto indicato nella sentenza del 2015, le Sezioni unite correttamente rilevano come nemmeno nella giurisprudenza della Corte europea dei diritti dell'uomo si possano trovare riscontri alla necessità di predeterminare l'ambiente di svolgimento delle operazioni di captazione.

In particolare l'art. 8 CEDU, di cui la sentenza *Musumeci* assumeva una violazione, non impone in realtà di indicare in via preventiva alcun luogo. Gli elementi richiesti per la compatibilità della disciplina interna sulle intercettazioni con la Convenzione EDU sono stati chiaramente identificati dalla giurisprudenza della Corte di Strasburgo, così come riassunti nella sentenza *Zakharov c. Russia* del 4 dicembre 2015, in tre parametri fondamentali: base giuridica appropriata, finalità legittima e necessità all'interno di una società democratica[16].

I presupposti per valutare come adeguata la base legale, anch'essi definiti da un orientamento consolidato, a loro volta comprendono: la predeterminazione della tipologia delle comunicazioni oggetto di intercettazione, la ricognizione dei reati per cui tali mezzi invasivi sono applicabili, l'attribuzione ad un organo indipendente della competenza ad autorizzare le intercettazioni, la definizione delle categorie di persone che possono essere interessate, dei limiti di durata e della procedura da osservare, l'utilizzazione e conservazione dei dati ottenuti e, da ultimo, l'individuazione dei casi in cui questi devono essere distrutti[17]. Appare quindi evidente come l'indicazione del luogo non figuri fra gli elementi necessari richiesti dalla Corte di Strasburgo, che, tra l'altro, ha recentemente ribadito la propria interpretazione in una decisione relativa al nostro ordinamento[18].

Correttamente, quindi, i giudici di legittimità concludono che la locuzione "ambientale" non costituisce un parametro normativo, ma esclusivamente un termine ampiamente diffuso in dottrina, giurisprudenza e nel linguaggio comune sulla base delle

---

[15] In tal senso, ad esempio, Cass., Sez. I, sent. 25 febbraio 2009, dep. 16 marzo 2009, n. 11506, Pres. Giordano, Rel. Bonito, Imp. Molè, C.E.D. 243044, secondo cui: «La intercettazione di comunicazioni tra presenti richiede – per come si desume chiaramente dal tenore dell'art. 266, secondo comma ult. parte C.P.P. – la indicazione dell'ambiente nel quale la operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indizione di cui all'art. 614 del codice penale». Sulla stessa linea anche Sez. II, sent. 8 aprile 2014, n. 17894, Alvaro, cit.

[16] Cfr. Corte EDU, *Zakharov c. Russia*, ricorso n. 47143/06, 4 dicembre 2015, § 227 ss.

[17] *Idem*, § 231 e la numerosa giurisprudenza precedente ivi citata.

[18] Cfr. Corte EDU, *Capriotti c. Italia*, ricorso n. 28819/12, 23 febbraio 2016, § 43- 44. A prescindere dai temi qui trattati, la sentenza è estremamente rilevante perché fornisce legittimità a quella prassi di intercettazioni telefoniche compiuta su suolo italiano ma relativa a comunicazioni effettuate all'estero, mediante il c.d. "instradamento".

tecniche di captazione disponibili in un determinato momento storico, quando l'uso di *software* a scopo di *surveillance* era ancora lungi dall'essere immaginato. All'epoca in cui venne scritta la normativa codicistica, infatti, vi era certamente coincidenza fattuale fra il concetto di intercettazione di comunicazioni "fra presenti" (cioè al di fuori del mezzo del telefono) e quello di intercettazione "ambientale", atteso che l'installazione dei dispositivi allora disponibili, tipicamente microspie, non poteva prescindere dalla loro collocazione in un preciso contesto fisico.

Da tale assimilazione puramente di fatto tuttavia, secondo le Sezioni unite, non può derivarsi a priori l'illegittimità delle intercettazioni svolte con dispositivi di captazione in grado di seguire il soggetto ovunque esso si trovi, e quindi tecnicamente impossibilitati (ad oggi, almeno) ad interrompere la registrazione in base al luogo in cui sono posti. D'altro canto, come già affermato dalla Corte costituzionale nella sentenza n. 135 del 2002, richiamata nella pronuncia in esame, nemmeno il riferimento all'art. 14 Cost. a "ispezioni, perquisizioni e sequestri" – forme di intrusione "palesi" – appare «necessariamente espressivo dell'intento di "tipizzare" le limitazioni permesse, escludendo a contrario quelle non espressamente contemplate»[19], né tali limitazioni all'uso di strumenti di captazione occulti possono riscontrarsi nell'art. 17 del Patto internazionale sui diritti civili e politici, o negli articoli 7 e 52 della Carta dei diritti fondamentali dell'Unione europea ("la Carta"). Non è quindi possibile invocare automaticamente una violazione della libertà di domicilio ogni qual volta il mezzo utilizzato non sia già previsto a livello legislativo, in quanto diventato disponibile «solo per effetto dei progressi tecnici successivi»[20].

3.3. La disciplina derogatoria del d.l. 152/1991.

Le Sezioni unite mettono inoltre in rilievo come la sentenza *Musumeci* abbia completamente tralasciato di tenere in considerazione la normativa speciale di cui all'art. 13 d.l. 152/1991, secondo la quale l'intercettazione all'interno del domicilio disposta «in relazione ad un delitto di criminalità organizzata» è consentita «anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa». Nell'ambito di applicazione del suddetto art. 13, quindi, le intercettazioni fra presenti possono essere disposte a prescindere dal luogo in cui devono essere sviluppate, consentendo esplicitamente allo Stato di utilizzare «tutti i mezzi che la moderna tecnologia offre». La Corte rileva infatti che, per tali delitti, il legislatore ha già operato uno specifico bilanciamento degli interessi in gioco, «optando per una più pregnante limitazione della segretezza delle comunicazioni e della tutela del domicilio tenendo conto della eccezionale gravità e pericolosità […] delle minacce che derivano alla società ed ai singoli delle articolate organizzazioni criminali che dispongono di sofisticate tecnologie e di notevoli risorse finanziarie».

---

[19] Corte Cost., sent. 11 aprile 2002, n. 135, § 2.1.

[20] *Idem*.

Di conseguenza, in questi casi, l'indicazione del luogo non può essere considerata elemento necessario del decreto di autorizzazione delle intercettazioni, nemmeno quando queste debbano svolgersi all'interno del privato domicilio.

3.4. I requisiti del decreto di autorizzazione delle intercettazioni "fra presenti".

Per i motivi sopra illustrati, la Corte condivide la tesi, già sostenuta dalla Sezione rimettente, secondo la quale l'utilizzo di un dispositivo informatico «"itinerante", con provvedimento di autorizzazione adeguatamente motivato e nel rispetto delle disposizioni generali in materia di intercettazione, costituisce una delle naturali modalità di attuazione delle intercettazioni al pari della collocazione di microspie». La necessità di indicare con precisione il luogo di svolgimento delle intercettazioni tra presenti non è richiesta né dalla legge, né dalla giurisprudenza nazionale o sovranazionale, salvo quando esse debbano avvenire in un domicilio privato. Nel caso in cui si proceda per i delitti di cui all'art. 13 d.l. 152/1991, tale presupposto non è mai necessario.

L'utilizzo di captatori informatici per i quali sia tecnicamente impossibile predeterminare gli ambienti dove le registrazioni avranno luogo deve quindi ritenersi legittimo, sulla base della normativa vigente, per le fattispecie a cui si applica la citata legge speciale.

Al contrario, la possibilità di porre in essere lo stesso tipo di intercettazioni «al di fuori della disciplina derogatoria di cui all'art. 13 della legge n. 203 del 1991» viene radicalmente esclusa, poiché in questo caso non si riuscirebbe a dare attuazione alla clausola prevista dall'art. 266 comma 2 c.p.p. a tutela del domicilio. Sotto questo profilo, la Corte non condivide la soluzione, indicata dalla Sezione rimettente, di sopperire in via successiva dichiarando l'inutilizzabilità di eventuali registrazioni effettuate in violazione dell'art. 14 Cost. all'interno della privata dimora. La funzione di questa invalidità processuale, infatti sarebbe, secondo le Sezioni unite, quella di rimediare occasionalmente a vizi che inficiano il materiale probatorio in astratto utilizzabile, e non invece di impedire l'ingresso nel processo di prove formate *contra legem* sin dalle origini. Tale sanzione in ogni caso, concludono pragmaticamente i giudici di legittimità, collocandosi in una fase successiva al deposito delle trascrizioni, non potrebbe comunque costituire una barriera efficace contro la possibile divulgazione dei contenuti delle intercettazioni, né una garanzia sufficiente nei procedimenti *de libertate*, quando il provvedimento restrittivo può basarsi anche sui soli brogliacci ai fini della gravità indiziaria.

3.5. L'ambito di applicazione della disciplina speciale: la definizione di "delitti di criminalità organizzata".

Da ultimo, le Sezioni unite riconoscono come, nel quadro appena delineato, la definizione di "criminalità organizzata" «non costituisce un mero esercizio teorico», perché da essa dipende l'applicazione delle norme processuali speciali.

La Corte rileva che l'individuazione dei reati inclusi in tale categoria non è mai stata effettuata in modo preciso dal legislatore, con il risultato che le disposizioni processuali che si riferiscono ai "delitti di criminalità organizzata" contenute nel codice o nelle disposizioni speciali talvolta si limitano ad indicare genericamente questa locuzione (fra cui ad esempio l'art. 13 d.l. 152/1991), talvolta invece enumerano una lista specifica di reati. Anche la seconda ipotesi, però, che comprende l'art. 51 comma 3-*bis* c.p.p.[21], l'art. 407 comma 2, lett. *a)* c.p.p.[22] e gli artt. 4-*bis* e 41-*bis* ord. pen.[23], non pare in grado di fornire parametri di riferimento certi, poiché ognuno di questi articoli prevede liste non omogenee di reati, in qualche caso anche a natura mono-soggettiva. Nemmeno a livello dottrinale, nonostante una certa convergenza in ambito sociologico, è mai stata trovata una definizione condivisa di "delitti di criminalità organizzata".

Sul punto, diversi orientamenti si sono susseguiti anche nella giurisprudenza di legittimità, che si è dapprima mostrata incline ad identificare il concetto di criminalità organizzata con i reati di cui all'art. 407 comma 2 lett. *a)* o di cui all'art. 51 comma 3-*bis* c.p.p., salvo optare successivamente per un approccio teleologico, riguardo alle finalità ricercate dalla disciplina speciale applicabile al caso concreto. In questo filone, si inserisce anche la pronuncia delle Sezioni unite *Petrarca* del 2005, secondo cui la locuzione "criminalità organizzata" deve essere intesa in modo ampio per includervi «non solo i reati di criminalità mafiosa e quelli associativi previsti da norme incriminatrici speciali, ma qualsiasi tipo di associazione per delinquere, *ex* art. 416 cod. pen., correlata alle attività criminose più diverse, con l'esclusione del mero concorso di persone del reato»[24]. In considerazione del particolare allarme sociale causato dalle strutture associative criminali le Sezioni unite, nella pronuncia in esame, ritengono di

---

[21] Riferito, in termini generali, ai delitti di cui agli artt. 416, comma 6 e 7, e 416, realizzato allo scopo di commettere delitti previsti dagli articoli 473 e 474, 600, 601, 602, 416-*bis*,416-*ter* e 630 c.p.; all'art. 74 d.p.r. 309/1990; all'art. 291-*quater* del d.p.r. 43/1973 (contrabbando di sigarette), e all'articolo 260 del d.l. 152/2006 (tutela dell'ambiente).

[22] Riferito, in termini generali, ai delitti di cui agli artt. 285, 286, 416, 416-*bis*, 422, 575, 628 comma 3, 629 comma 2, 630, 270 comma 3, 306 comma 2, 600, 600-*bis* comma 1, 600-*ter* comma 1 e 3, 601, 602, 609-*ter*, 609-*quater*, 609-*octies* c.p.; art. 291-*ter*, comma 2 lett. *a), d) ed e)* e 291-*quater*, comma 4, d.p.r. 43/1973; ai delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale; agli artt. 73 e 80, comma 2, e 74 d.p.r. 309/1990; art. 12 comma 3 d.lgs 286/1998 e ai delitti legati al commercio di armi da guerra.

[23] Riferiti, in termini generali, agli artt. 575, 628, comma 3, 629, comma 2, 416, 416-*bis*, 609-*bis*, 609-*quater*, 609-*quinquies*, 609-*octies*, 630 c.p. ; ai delitti commessi per finalità di terrorismo o di eversione dell'ordinamento costituzionale; agli art. 291-*ter* e *quater* d.p.r. 43/1973; e agli artt. 80 comma 2 e 74 d.p.r. 309/1990.

[24] Sez. un., 22 marzo 2005, dep. 11 maggio 2005, n. 117706, Pres. Marvulli, Rel. Fiale, Imp. Petrarca e a., in *Cass. pen.*, 2005, p. 2916 con nota di MELILLO, *Appunti in tema di sospensione feriale dei termini relativi a procedimenti per reati di criminalità organizzata*, e commentata anche da LEO, *La nozione processuale di criminalità organizzata*, in *Corr. mer.*, 2005, p. 830.

richiamarsi a quest'ultima definizione, considerata la più adatta a cogliere l'essenza di un delitto di criminalità organizzata e le *rationes* ispiratrici delle discipline derogatorie approvate dal legislatore.

4. La necessaria neutralità tecnica delle intercettazioni tra presenti.

La sentenza in commento presenta un'apprezzabile opera di ricostruzione dei presupposti delle intercettazioni tra presenti, che affranca il mezzo di ricerca della prova previsto dall'art. 266 comma 2 c.p.p. dalla tradizionale definizione di "intercettazione ambientale" legata alle tecnologie utilizzate quando la legislazione in materia di intercettazioni era stata introdotta nel nostro ordinamento.

Sotto questo profilo, la pronuncia delle Sezioni unite sembra abbracciare il principio di "neutralità tecnica" della disciplina positiva del fenomeno, principio già affermato a livello europeo in materia di protezione dei dati personali, secondo la quale la normativa dovrebbe trovare applicazione a prescindere dalla tecnologia utilizzata per ottenere un determinato scopo. Questa neutralità tecnica non deve comunque essere intesa come una impropria e pericolosa legittimazione in via giurisprudenziale di qualsiasi mezzo di indagine, anche se altamente intrusivo.

Innanzitutto, come correttamente ricostruito dai giudici di legittimità, la necessità di indicare dello strumento tramite cui effettuare le intercettazioni non trova giustificazione nell'attuale sistema codicistico che peraltro, all'art. 268 comma 3 c.p.p., anche rispetto alle intercettazioni telefoniche "tradizionali", è ben lungi dall'essere tassativo quando richiede genericamente di fare uso solo degli «impianti installati nella procura della Repubblica», conferendo inoltre facoltà al pubblico ministero, con un mero provvedimento motivato, di optare altrimenti.

Invero, il rispetto della doppia riserva di legge e di giurisdizione richiesta dalla Costituzione per ogni tipo di intrusione nelle libertà fondamentali poste a tutela del domicilio privato e delle comunicazioni non si estende – nel quadro normativo vigente – anche alla necessità di avere una specifica previsione legislativa per ogni tipologia di strumento captativo utilizzabile. In questo senso, bene hanno fatto i giudici di legittimità a ricordare come la Corte costituzionale abbia già riconosciuto che l'art. 14 Cost. non debba essere inteso in senso restrittivo rispetto ai mezzi di ricerca della prova ivi indicati. Tra l'altro, come sottolineato dalla Procura generale nella memoria depositata per il procedimento davanti alle Sezioni unite, appoggiare un'interpretazione in questo senso significherebbe giungere al risultato paradossale di conferire al domicilio una protezione maggiore di quella prevista per la libertà personale di cui all'art. 13 Cost., che contiene una clausola di chiusura ampia e riferita a «qualsiasi altra restrizione della libertà persona»[25]. Non può quindi ragionevolmente nemmeno sostenersi che alle

[25] Procura generale presso la Corte di cassazione, *Memoria per la camera di consiglio delle Sezioni Unite del 28 aprile 2016*, p. 13, pubblicata in *questa Rivista* insieme al relativo allegato.

intercettazioni effettuate a mezzo di captatore informatico possa applicarsi la categoria delle cosiddette prove "incostituzionali"[26].

Queste conclusioni assumono uno specifico peso alla luce dei principi ispiratori della nuova normativa europea emanata in materia di protezione dei dati personali[27]. La Direttiva 2016/680 prende infatti esplicitamente in considerazione le sfide poste dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione, e le potenzialità intrusive che queste rappresentano, «come mai in precedenza», contro la tutela delle informazioni più sensibili dell'individuo, con particolare riferimento ad «attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali»[28]. Sotto questo profilo, il legislatore europeo sottolinea esplicitamente che «al fine di evitare che si corrano gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate»[29]. Anche sulla base di tale orientamento, seppure sviluppato in un diverso contesto, le affermazioni della Corte di cassazione sull'utilizzabilità dei *Trojans* come strumenti di *surveillance,* pur in assenza di una specifica previsione normativa, possono essere considerate del tutto legittime.

---

[26] A favore di questa tesi, ad esempio TESTAGUZZA, *I sistemi di controllo remoto,* cit., p. 761; TORRE, *Il* virus *di Stato,* cit., p. 1167. Il concetto di prova incostituzionale, riconosciuto dalla Corte costituzionale a partire dalla sentenza 6 aprile 1973, n. 34, si riferisce alla «prova assunta con modalità lesive dei diritti fondamentali del cittadino garantiti dalla Costituzione»: sul tema, cfr. GREVI, *Insegnamenti, moniti e silenzi della Corte Costituzionale in tema di intercettazioni telefoniche*, in *Giur. cost*., 1974, p. 341. Sulla distinzione fra prova illecita e prova incostituzionale, si vedano COMOGLIO, *Perquisizione illegittima ed inutilizzabilità derivata delle prove acquisite con il susseguente sequestro*, in *Cass. pen*., 1996, p. 1549; CAPRIOLI, *Colloqui riservati e prova penale*, Torino, 2000, p. 236. La configurabilità delle prove incostituzionali è stata a lungo oggetto di dibattito. Per l'orientamento favorevole a riconoscere invalidità processuali anche al di fuori del codice di procedura in caso di contrasto con le garanzie costituzionali, si vedano ad esempio GREVI, cit., p. 341 e, per lo meno in quanto la Costituzione contenga norme processuali sufficientemente precise, ILLUMINATI, *L'inutilizzabilità della prova nel processo penale*, in *Riv. it. dir. proc. pen*., 2010, p. 521; ID., *La disciplina processuale delle intercettazioni*, Giuffrè, 1983, p. 138 ss. Sull'applicazione di questa categoria in tema di dati personali si veda anche CAMON, *Le riprese visive come mezzo di indagine: spunti per una riflessione sulle prove "incostituzionali"*, in *Cass. pen*., 1999, p. 1206. Fra le posizioni contrarie alla possibilità di riconoscere una sanzione processuale in mancanza di una specifica invalidità processuale, si vedano invece CORDERO, Tre studi sulle prove penali, Giuffré, 1963, p. 154 e ss.; ID., Procedura penale, 2012, IX ed., Giuffré, p. 639; GALANTINI, voce *Inutilizzabilità (dir. proc. pen.)*, in *Enc. Dir. Agg. I*, Milano, 1997, p. 699.

[27] Intesi come «qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica», cfr. art. 3(1) Direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio.

[28] Cfr. considerando (3) Direttiva 2016/680; si veda anche considerando (7) che auspica una maggiore applicazione di questi principi anche alla materia penale e nel campo della cooperazione giudiziaria.

[29] Cfr. considerando (18), Direttiva 2016/680.

Questo non deve tuttavia immediatamente far temere un abbassamento dei livelli di tutela posti a presidio dei diritti e delle libertà fondamentali dell'individuo (e dell'indagato). In questo ambito, infatti, una legislazione tassativa rischia di non essere sempre la modalità più adeguata per ottenere un livello di protezione consono ai valori costituzionali in gioco. In particolare, circoscrivere l'applicazione della normativa solo a determinati strumenti captativi (presumibilmente quelli più diffusi in un certo momento storico) quando si ha a che fare con attività soggette a continua evoluzione tecnologica, rischia di condannare la legge a nascere sorpassata in partenza.

L'esclusione *in toto* di queste tecnologie dal novero degli strumenti di indagine penale sarebbe un'opzione che, oltre ad essere totalmente anacronistica, non tiene conto dell'ampio utilizzo degli stessi mezzi da parte di organizzazioni criminali e che lascerebbe alle forze dell'ordine solo l'uso di tecnologie tendenzialmente superate o facilmente aggirabili[30].

Del resto appare inutile giocare sull'assenza di una normativa certa. Come l'esempio statunitense e le recenti cronache nel vecchio continente hanno mostrato[31], la mancanza di una base legale chiara non ha impedito, né impedisce, di fatto, l'uso di nuove forme di *surveillance* all'interno dei sistemi statali e in particolare durante le indagini penali, ma certamente lascia l'indagato sprovvisto di un quadro normativo certo dove far valere i propri diritti.

La "neutralità tecnica" richiesta dalla Direttiva 2016/680 appare, in definitiva, l'approccio preferibile per regolare forme diverse di tecnologie. Sarebbe quindi auspicabile un intervento legislativo che identificasse chiaramente non tanto tutte le singole tecnologie utilizzabili nel campo delle intercettazioni (che prima erano microspie, oggi sono *virus* informatici, ma potrebbero ovviamente a breve avere anche forma ben diversa), quanto piuttosto le garanzie fondamentali che devono sempre essere riconosciute all'indagato e ai soggetti terzi potenzialmente coinvolti, a prescindere dallo strumento utilizzato[32].

Un esempio lampante di come un intento, certamente condivisibile, come quello della certezza del diritto possa tradursi – se espresso attraverso la tipicità degli strumenti, in un ambito come quello in oggetto – in una compressione dei diritti dell'indagato, è dato dall'uso di captatori informatici per l'acquisizione di flussi di dati. In mancanza di una specifica norma di riferimento, ad oggi la giurisprudenza ha classificato questa tecnica investigativa come un mezzo di ricerca della prova atipico, utilizzabile con un mero provvedimento motivato del pubblico ministero, senza alcun

---

[30] Opzione invece considerata necessaria, in assenza di perfetta assimilazione della fattispecie in esame ai casi di perquisizione, da TESTAGUZZA, *I sistemi di controllo remoto,* cit., p. 766.

[31] Si vedano, ad esempio, *Cybersicurezza, svelata la piattaforma di spionaggio Sauron*, in *La Repubblica*, 29 agosto 2016 e SOGHOIAN, *DOJ's 'Hotwatch' Real-Time Surveillance of Credit Card Transactions*, 4 dicembre 2010.

[32] In tal senso, anche l'apprezzabile e compiuta descrizione effettuata dalle Sezioni unite delle potenzialità intrusive dei *Trojan* non deve essere intesa come riconoscimento della legittimità ad effettuare intercettazioni informatiche solo con questo specifico tipo di captatore (peraltro già costituente una categoria piuttosto ampia di software).

coinvolgimento del giudice per le indagini preliminari[33]. Come già riconosciuto non solo da parte della dottrina, ma anche da alcuni degli stessi organi inquirenti[34], l'impossibilità o forse la reticenza, ad applicare categorie normative tecnologicamente orientate a nuove forme di captazione, non meno invasive delle intercettazioni "tradizionali" (comportando anch'esse un controllo in tempo reale sulla sfera personale dell'individuo), si è risolta in una notevole riduzione delle garanzie a tutela dell'indagato.

Anche in tal senso, si dovrebbe quindi invocare un intervento legislativo non per includere espressamente ogni specifico mezzo di *surveillance*, quanto piuttosto per disciplinare in modo generale, dal punto di vista dei diritti, tutti i fenomeni di captazione di flussi di informazioni (comunicative e non) in tempo reale. Peraltro, la possibilità, riconosciuta anche dalle Sezioni unite, di utilizzare gli stessi captatori informatici sia per l'intercettazione di dati che per quella di comunicazioni probabilmente già rende (e sempre più renderà) difficile continuare a richiedere forme di tutela tanto differenziate a seconda dell'oggetto della captazione[35].

Più precisamente, sebbene il tema non sia stato esplicitamente trattato nella sentenza in oggetto, a parere di chi scrive il sistema costituzionale della riserva di legge e di giurisdizione dovrebbe diventare il paradigma normativo per tutte le forme di controllo da remoto sui dati personali effettuate in tempo reale. Ciò dovrebbe comportare un'estensione delle garanzie procedurali previste dalla disciplina delle intercettazioni anche all'acquisizione di dati futuri o "in formazione". La suggerita applicazione di una disciplina comune per tutte le forme di *surveillance* richiede ovviamente il riconoscimento di un bene costituzionale che estenda la propria tutela a tutte le informazioni riservate, a prescindere dalla loro forma (dati o comunicazioni) e dal mezzo attraverso cui vengono espresse (uso del telefono, del computer o di altro dispositivo). Un nuovo ed ampio concetto di "dati personali"[36] pare quindi necessario per includere anche una protezione dello spazio "virtuale" della persona che, come

---

[33] Cfr. ad esempio Cass., sent. 14 ottobre 2009, n. 16556, Virruso, cit., p. 20.

[34] In questo senso si veda, ad esempio, ATERNO, *Le investigazioni informatiche,* cit., par. 2; CAIANIELLO, *Increasing Discretionary Prosecutor's Powers: The Pivotal Role of the Italian Prosecutor in the Pretrial Investigation Phase*, in *Oxford Handbooks Online*, aprile 2016. La necessità di utilizzare le garanzie tipiche delle intercettazioni anche per la captazione in tempo reale di flussi di dati era stata sollevata anche dai sostituti procuratori nel c.d. "caso Bisignani", ma la possibilità era stata negata dal giudice per le indagini preliminari in carica, cfr. TORRE, *Il* virus *di Stato*, cit., p. 1167.

[35] Cfr. anche TORRE, *Il* virus *di Stato*, cit., p. 1165-1166. Come similmente apparirà sempre più difficile la distinzione fra videoriprese a contenuto comunicativo e non comunicativo, pure affermata dalle Sezioni unite con sent. 28 marzo 2006, dep. 28 luglio 2006, n. 26795, Pres. Marvulli, Rel. Lattanzi, Imp. Prisco, in *Dir. pen. e proc*., 2006, p. 1347, con nota di CONTI, *Le video-riprese tra prova atipica e prova incostituzionale: le Sezioni Unite elaborano la categoria dei luoghi "riservati"*, nonché in *Cass. pen*., 2006, p. 3937, con nota di RUGGERI, *Riprese visive e inammissibilità della prova*; commentata anche da BELTRANI, *Le videoriprese? Sono una prova atipica*, in *Dir. e giust*., 2006, p. 40.

[36] Affermatasi sin dalla Convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati a caratteri personali, STE n. 108.

correttamente rilevato[37], non può essere del tutto omologato alla tutela conferita ad altre libertà, ad esempio a quella della privata dimora, senza incorrere in evidenti forzature[38].

In tal senso, un esempio fondamentale viene dalla ormai nota sentenza della Corte Costituzionale tedesca del 2008, confermata nel 2016 con esplicito riferimento all'uso di *Trojans*[39], con la quale è stata riconosciuta l'inadeguatezza dei diritti a tutela delle libertà di domicilio e delle comunicazioni a dare copertura sufficiente allo spazio digitale, e ed è stato inaugurato un nuovo diritto costituzionale «alla garanzia dell'integrità e della riservatezza dei sistemi informatici», fondato sulla dignità umana dell'individuo e dell'utente "informatico"[40].

Una simile operazione può e deve essere urgentemente effettuata anche nel nostro ordinamento, come del resto sta accadendo anche in numerosi sistemi giuridici europei[41]. A questo fine, forse, non è necessaria alcuna riforma costituzionale: come evidenziato, un «nuovo diritto fondamentale all'uso riservato delle tecnologie informatiche» potrebbe essere enucleato, anche dalla Corte costituzionale a partire dall'art. 2 Cost., che già è clausola di ingresso nel nostro ordinamento dei diritti inviolabili della persona non altrimenti espressamente previsti[42]. In questo caso, tuttavia, a ben vedere, dal dettato costituzionale sarebbe difficile far discendere automaticamente la necessità di rispettare – anche nel caso di captatori informatici omnicomprensivi – la riserva di legge e di giurisdizione prevista espressamente negli artt. 13, 15 e 15 Cost. Un'altra strada deriva invece direttamente dall'applicazione della giurisprudenza delle Corti europee. Da tempo, l'interpretazione consolidata della Corte EDU ha fatto rientrare nella protezione del diritto alla "vita privata" di cui all'art. 8 CEDU tutto l'ambito dei dati personali in cui si esplica la personalità individuale, componenti

---

[37] ORLANDI, *Osservazioni sul Documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Archivio pen.*, 25 luglio 2016; ID., *La riforma del processo penale fra correzioni strutturali e tutela "progressiva" dei diritti fondamentali*, in *Riv. it. dir. e proc. pen.*, 2014, p. 1133-1164.

[38] Per le quali si è ad esempio giunti a tutelare i dati contenuti nel computer quando questo si trova all'interno del domicilio, ma non quando questo si trovi in luoghi pubblici, prescindendo totalmente dalla circostanza fattuale che – ad esempio tramite l'accesso al *cloud* – il soggetto potrebbe in entrambi i casi compiere in entrambi i luoghi attività con il medesimo livello di sensibilità, cfr. Cass., sent. 14 ottobre 2009, n. 16556, Virruso, cit., p. 20-21.

[39] Bundersverfassungsgericht, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09, con nota di GIORDANO - VENEGONI, *La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici*, in *questa Rivista*, 8 maggio 2016.

[40] Bundesverfassungsgericht, 27 febbraio 2008, BVerfGE 120, 274 ss., in *Riv. trim. dir. pen. econ.*, 2009, p. 679 ss., con nota di FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*; sul punto si veda anche ORLANDI, *Questioni attuali in tema di processo penale e informatica*, in *Riv. dir. proc.*, 2009, p. 129 ss.

[41] Quali ad esempio, oltre alla già citata Germania, anche Spagna (Ley Orgánica 13/2015) e Francia (sia nell'attuale codice di procedura penale, sia nella proposta di riforma attualmente in discussione). Per un sommario delle disposizioni rilevanti si rimanda all'allegato della memoria depositata dalla Procura Generale.

[42] In questo senso la sentenza in commento, p. 21, riprendendo quanto affermato nella Memoria depositata dalla Procura Generale, p. 18; sul punto anche ORLANDI, *Osservazioni*, cit.

"virtuali" e "comunicative" incluse[43]. Ne consegue che l'intercettazione e la memorizzazione di tali dati, nonché il loro eventuale uso nell'ambito dei procedimenti penali, rientra sempre nel campo di protezione del diritto al rispetto della vita privata e familiare, a prescindere dal mezzo tecnico utilizzato. In virtù dell'art. 52(3) della Carta, simile contenuto viene peraltro riconosciuto anche ai diritti tutelati dagli articoli 7 e 8 dello stesso testo, così come interpretati dalla Corte di giustizia nel *leading case Digital Rights Ireland Ltd*[44].

Tuttavia, mentre si ritiene condivisibile la sentenza in esame dove afferma che l'estensione della disciplina delle intercettazioni anche ai nuovi strumenti captativi può effettuarsi direttamente in via interpretativa rispetto ai dati personali comunicativi, l'estensione del regime di tutela costituzionale all'acquisizione di flussi di informazioni potrebbe essere effettuata solo con l'intervento del legislatore, ad esempio modificando l'art. 266-*bis* c.p.p. per includervi non solo l'intercettazione di "comunicazioni" ma anche di "dati"[45]. Esclusivamente sotto questo secondo profilo, si concorda quindi con quella dottrina secondo cui tali forme di indagini dovrebbero essere considerate del tutto illegittime ed inutilizzabili, nel nostro ordinamento, se realizzate sotto l'incerta e insufficiente tutela fornita dall'attuale regime processuale delle prove atipiche[46].

5. L'irrilevanza dell'indicazione del luogo ai fini della legittimità delle intercettazioni.

In attesa di un tale intervento legislativo ed alla luce del quadro normativo vigente, la ricostruzione dei presupposti per le intercettazioni fra presenti effettuata dalle Sezioni unite con la sentenza in esame ha apportato la necessità di non più rinviabile aggiornamento degli strumenti di indagine penale previsti dall'attuale codice di procedura.

In particolare, apprezzabile è la chiarezza con cui la Corte ha sottolineato l'assenza di basi legali per sostenere che la predeterminazione del luogo di svolgimento delle intercettazioni sia un requisito richiesto a pena di inutilizzabilità dalla legge, dalla giurisprudenza o dalla Costituzione[47]. Questa affermazione ha infatti il pregio di

---

[43] Cfr., fra le molte, *X v. The Federal Republic of Germany*, 7 maggio 1981, ricorso n. 8334/78. Da ultimo, si veda *Capriotti c. Italia*, cit., § 43 e la giurisprudenza ivi citata.

[44] Corte di giustizia dell'Unione europea, Cause riunite C293/12 e C594/12, 8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána*, § 52-54.

[45] Atteso che il concetto di "intercettazione di comunicazioni" appare al momento solidamente definito al concetto di dialogo fra soggetti a seguito della sentenza *Torcasio*, cfr. Cass., Sez. un., 28 maggio 2003, dep. 24 settembre 2003, n. 36747, Pres. Marvulli, Rel. Milo, Imp. Torcasio, in *Cass. pen.*, 2004, p. 2094 con nota di FILIPPI, *Le Sezioni Unite decretano la morte dell'agente segreto "attrezzato per il suono"*; commentata anche da FUMU, *Registrazione di colloqui tra presenti effettuata a cura della polizia giudiziaria: insuperabili i limiti alla testimonianza indiretta*, in *Riv. pol.*, 2003, p. 762. Sul punto si veda anche ILLUMINATI, *La disciplina processuale delle intercettazioni*, cit., p. 27.

[46] Cfr. ORLANDI, *Osservazioni*, cit.; TESTAGUZZA, *I sistemi di controllo remoto*, cit., p. 766.

[47] In tal senso, non sembra invece che la giurisprudenza in materia di variazioni del luogo, citata a supporto di tesi opposte sia nella sentenza *Musumeci* sia nelle due pronunce *Scurato*, possa fornire un elemento

riconoscere la necessità di non confinare l'applicazione della disciplina delle intercettazioni ad uno specifico strumento di captazione ad installazione "fissa" (come le microspie), ma di aprire il sistema delle indagini penali ad una tutela dei diritti tecnicamente neutra.

Tale conclusione non porta certamente a ritenere utilizzabili in modo indiscriminato forme di intercettazione lesive del diritto alla riservatezza del domicilio in ogni contesto, come viene sottolineato dagli stessi giudici di legittimità. Le conclusioni prospettate dalle Sezioni unite, tuttavia, trovano immediata applicazione nella disciplina speciale di cui all'art. 13 d.l. 152/1991, che chiaramente afferma l'indifferenza della collocazione spaziale delle intercettazioni, e la cui omessa considerazione costituisce il principale elemento di fragilità della sentenza *Musumeci*, ma non solo di questa decisione. Apparentemente, tale disciplina e la conseguente differenza fra i requisiti richiesti quando si proceda per un delitto "comune" rispetto ad uno di "criminalità organizzata", non sembra mai essere stata presa in considerazione nemmeno negli altri casi citati in materia di *surveillance* e affrontati precedentemente dalla giurisprudenza di legittimità e di merito, pure tutti riferibili ai delitti di cui agli artt. 416 e 416-*bis* c.p.[48].

Nell'ambito di applicazione della normativa speciale, sollevare il giudice e il pubblico ministero dalla necessità di indicare preventivamente il luogo dove si svolgeranno le intercettazioni contribuisce a rendere più trasparente la richiesta – e nell'autorizzazione, la necessità – di realizzare forme di controllo omnicomprensive, sia per gli strumenti tecnici utilizzati sia per il coinvolgimento di numerosi soggetti che pongono in essere multiple e diversificate forme comunicative. In questo senso, è possibile evitare di ricorrere a finzioni giuridiche di facciata che non consentono in realtà alcuna tutela sostanziale all'indagato, quali l'indicazione della "stanza" o del "luogo in cui è ubicato"[49] il dispositivo e che, al di là del dato testuale, chiaramente alludono a forme di controllo che prescindono da limiti spaziali determinati. Altrettanto imprecisi, sia sul piano tecnico sia su quello della certezza del diritto, appaiono anche quei parametri che rimettono la definizione dell'ambiente di captazione al raggio entro cui lo specifico mezzo utilizzato può registrare a distanza, atteso che al momento non pare esserci una definizione sufficientemente condivisa delle effettive qualità tecniche dei vari dispositivi sul mercato.

La possibilità di porre in essere forme di *surveillance* più intrusive in relazione a reati di particolare gravità, d'altro canto, trova riscontro anche nel quadro convenzionale. Come indicato dalle Sezioni unite, infatti, la Corte di Strasburgo ha

---

decisivo al dibattito. In particolare, mentre da un lato questa può essere utile per rigettare l'idea di un luogo rigidamente predeterminato, dall'altro la specificità dei casi in materia (tutti riferiti a carceri o veicoli) limita in parte la possibilità di usarla come base giuridica determinante su cui fondare i presupposti delle intercettazioni fra presenti.

[48] Né da parte di alcuna dottrina che di tali pronunce si è occupata, così ad esempio LORENZETTO, *Il perimetro delle intercettazioni ambientali*, cit., secondo cui i principi costituzionali e sovranazionali «impongono la rigorosa interpretazione dell'art. 266 comma 2 c.p.p., mettendo a rischio i risultati dell'intercettazione ambientale ove manchi la predeterminazione dei luoghi in cui si svolgono le operazioni»; sulla stessa linea anche TESTAGUZZA, *I sistemi di controllo remoto,* cit., p. 761.

[49] Trib. Palermo, Sez. riesame, ord. 11 gennaio 2016, cit., p. 3.

chiaramente identificato nella propria giurisprudenza i requisiti minimi per la legittimità di una normativa nazionale in tema di intercettazioni senza includervi l'indicazione del luogo.

Per la verità, nella sentenza *Zakharov c. Russia*[50] il parametro del luogo viene, in certa misura, preso in considerazione dalla Corte, sebbene con riferimento piuttosto generico all'«insieme dei luoghi» interessati da intercettazioni e non invece all'indicazione precisa dell'ambiente in cui la captazione deve essere sviluppata. Anche così configurato, tuttavia, l'elemento topografico può dirsi comunque irrilevante ai fini del tema trattato, poiché richiesto dalla Corte solo in via secondaria ed alternativa all'identificazione del soggetto che deve essere sottoposto ad intercettazioni[51]. In pratica, secondo la giurisprudenza di Strasburgo, se la persona (l'indagato o soggetto terzo) interessata dalla misura di *surveillance* è chiaramente indicata nel decreto di autorizzazione, non è necessario specificare l'ambiente in cui la captazione deve svilupparsi[52]. Non sembra quindi appropriato, per lo meno allo stato attuale, invocare l'art. 8 CEDU per sostenere la necessità di specificare l'indicazione del luogo ai fini della legittimità dell'intercettazione.

Ritenere inutile l'indicazione del luogo per taluni reati di particolare gravità – per effettiva mancanza di basi legali – non significa tuttavia automaticamente ridurre i diritti dei soggetti affetti da questo tipo di misure. Come infatti si dirà più avanti, l'uso della tecnologia informatica nel campo delle indagini penali deve certamente essere bilanciata da adeguate e specifiche garanzie per tutelare i diritti e le libertà fondamentali dei cittadini.

6. Le fattispecie sostanziali selezionate dalla Corte.

Il punto forse più controverso dell'intera pronuncia in esame si riscontra nella scelta compiuta dalle Sezioni unite rispetto all'ambito di applicazione della disciplina speciale di cui al d.l. 152/1991.

Sotto questo profilo, non risultano di particolare aiuto le normative sovranazionali citate dalla sentenza[53] cui potrebbe anche aggiungersi la Convenzione di

---

[50] E nei casi che l'hanno preceduta, si veda ad esempio Corte EDU, *Vetter c. Francia*, 31 maggio 2005, ricorso n. 59842/00; *Kennedy c. Regno Unito*, 18 maggio 2010, ricorso n. 26839/05.

[51] Cfr. Corte EDU, *Zakharov c. Russia*, cit., § 264.

[52] Tale orientamento ha trovato conferma anche nella recente sentenza *Capriotti c. Italia*, cit., § 39-44 ss.

[53] Cfr. art. 1, Azione Comune adottata il 21 dicembre 1998 dal Consiglio dell'Unione europea sulla base dell'art. K.3 del Trattato sull'Unione europea, relativa alla punibilità della partecipazione a un'organizzazione criminale negli Stati membri dell'Unione europea; art. 8 legge 22 aprile 2005, n. 69 "Disposizioni per conformare il diritto interno alla decisione quadro 2002/584/GAI del Consiglio, del 13 giugno 2002, relativa al mandato d'arresto europeo e alle procedure di consegna tra Stati membri"; art. 1, Decisione quadro 2008/841/GAI del Consiglio del 24 ottobre 2008 relativa alla lotta contro la criminalità organizzata; Risoluzione del Parlamento europeo del 25 ottobre 2011 sulla criminalità organizzata nell'Unione europea (2010/2309(INI)); Parlamento europeo, Documento di lavoro sulla Criminalità Organizzata, Commissione speciale sulla criminalità organizzata, la corruzione e il riciclaggio di denaro

Palermo del 2000[54], che, occupandosi del tema, forniscono definizioni talvolta più specifiche, talvolta più generiche ma mai del tutto sovrapponibili.

Allo stesso tempo, come evidenziato dai giudici di legittimità, la definizione di "delitto di criminalità organizzata" risulta effettivamente carente nella legislazione interna. Gli elenchi di reati contenuti negli articoli 51 comma 3-*bis* e 407 comma 2 lett. *a)* c.p.p. sono stati notevolmente modificati ed ampliati nel corso degli anni, e contengono ad oggi un insieme piuttosto eterogeneo di delitti, selezionati sulla base di criteri non sempre chiaramente identificabili almeno nel loro risultato finale (ad esempio può apparire paradossale che i reati di contraffazione di segni distintivi previsti agli art. 473 e 474 c.p. siano inclusi negli elenchi di reati "gravi", mentre altri delitti di almeno pari gravità, come quelli contro la pubblica amministrazione o i beni culturali e il paesaggio, non vengano menzionati).

Da ultimo, indicazioni precise in termini di fattispecie sostanziali non possono derivarsi neanche dalla giurisprudenza EDU, che nemmeno per la normativa nazionale in tema di intercettazioni "ordinarie" richiede un'elencazione tassativa di tutte le ipotesi criminose, purché siano forniti sufficienti dettagli sulla natura dei reati (ad esempio con l'indicazione del massimo della pena prevista[55]).

Un intervento legislativo sul punto appare quindi estremamente opportuno, per sottrarre scelte prettamente di politica criminale alla discrezione delle corti (che però in assenza di un quadro normativo preciso sono costrette ad esprimersi anche su questo punto, esponendosi a diverse critiche[56]) e dare piena legittimazione democratica all'inclusione o meno di determinate fattispecie nella categoria dei delitti di criminalità organizzata, con una scelta consapevole e non solo data dal mancato coordinamento di normative sviluppate in diversi periodi storici.

Al di là di questo – fondamentale – aspetto, il d.l. 152/1991 presenta un altro profilo sostanziale rilevante, che non è stato preso in considerazione nella pronuncia in esame. La disciplina derogatoria rispetto alle intercettazioni fra presenti tipiche, infatti, non è limitata ai soli delitti di criminalità organizzata. Da un lato, infatti, la riforma del 2003 sulle misure "contro la tratta di persone" ha già esteso l'art. 13 anche ai delitti di

---

(Relatore: Salvatore Iacolino), 1 ottobre 2012; Risoluzione del Parlamento europeo del 23 ottobre 2013 sulla criminalità organizzata, la corruzione e il riciclaggio di denaro: raccomandazioni in merito ad azioni e iniziative da intraprendere (relazione finale) (2013/2107(INI)).

[54] Convenzione delle Nazioni Unite contro la criminalità organizzata transnazionale, sottoscritta nel corso della Conferenza di Palermo (12 - 15 dicembre 2000) e adottata dall'Assemblea generale con risoluzione 55/25 del 15 novembre 2000; ratificata in Italia con legge n. 146 del 16 marzo 2006.

[55] Cfr. Corte EDU, *Zakharov c. Russia*, cit., § 231.

[56] Ad esempio, la Procura generale, nella Memoria depositata per la camera di consiglio, ha criticato anticipatamente la scelta di uniformarsi alla definizione formulata dalle Sezioni unite *Petrarca*, che si è pronunciata non nel campo dell'applicazione delle intercettazioni, ma in quello, meno "sensibile" della sospensione dei termini processuali in periodo feriale *ex* art. 240-*bis*, comma 2 disp. coord. c.p.p., sostenendo la scorrettezza di effettuare "meccaniche traslazioni" in questo ambito. Similmente, non appare particolarmente motivata la scelta della Corte di optare per la lista di delitti prevista dall'art. 51 (che ad esempio non include i delitti in materia di atti sessuali con minorenni) piuttosto che per quella indicata dall'art. 407 c.p.p.

sfruttamento della prostituzione e contro la personalità individuale[57]. Dall'altro, l'art. 13 si applica testualmente anche ai delitti "di minaccia col mezzo del telefono".

Anche per tali reati dovrebbe quindi ragionevolmente riconoscersi la possibilità di effettuare intercettazioni a mezzo di captatori informatici a prescindere dall'indicazione del luogo nel decreto di autorizzazione. Su questo punto ci si potrebbe anche spingere un poco oltre: applicando lo stesso parametro "storico" identificato dalle Sezioni unite sulla espressa inclusione di determinate tecnologie nel testo normativo, forse una lettura aggiornata dell'art. 13 richiederebbe di estendere l'espressione "delitti di minaccia col mezzo del telefono" anche a quelli commessi con mezzi informatici, primi fra tutti i cosiddetti *cybercrimes*[58]. Potrebbe infatti apparire paradossale che, solo a causa di disposizioni legislative non "tecnicamente neutrali", strumenti investigativi tecnologicamente avanzati non si possano utilizzare proprio per contrastare chi, tramite gli stessi mezzi, mira ad ottenere fini illeciti[59]. A tal fine, tuttavia, un intervento legislativo risulta necessario, non essendo possibile compiere una simile estensione in via interpretativa.

7. Nuovi strumenti e nuove tutele.

Si è già argomentato che, a fronte all'avanzare di nuove tecnologie, la soluzione praticabile non può essere quella di escluderne *in toto* l'applicazione, esplicitamente o indirettamente, dall'ambito giuridico e processuale. In particolare, l'apertura del sistema delle indagini penali in Italia a forme di intercettazioni effettuate tramite captatori informatici omnicomprensivi rappresenta un passo necessario nell'attuale contesto storico, dove queste forme di *surveillance* vengono ormai di fatto esercitate.

Questo riconoscimento richiede ovviamente un adeguato rafforzamento delle garanzie poste a tutela dei soggetti interessati dalle intercettazioni, sia in quanto indagati[60], sia in quanto soggetti terzi. In questo senso, le riserve costituzionali e le garanzie previste dalla disciplina codicistica delle intercettazioni forniscono certamente un elemento imprescindibile di tutela che non deve venire meno. Le tecnologie informatiche, tuttavia, richiedono anche ulteriori forme di protezione, non solo di natura giuridica, il cui rispetto dovrebbe però essere tutelato dalla legge, da applicarsi soprattutto in via preventiva in ossequio a criteri di proporzionalità. Questo principio, infatti, sta assumendo un ruolo sempre più fondamentale quale condizione di legittimità

---

[57] Cfr. art. 9, l. 11 agosto 2003, n. 228.

[58] Cfr. *Convenzione sul cybercrime*, Budapest, 23 novembre 2001, STE n. 185, recepita nell'ordinamento UE con la Direttiva 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013 relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio.

[59] Una simile estensione è già stata riconosciuta ad esempio nell'ordinamento spagnolo a seguito della riforma del 2015 (cf. art. 588-ter a del codice di procedura penale spagnolo, riportato anche nell'allegato della Memoria depositata dalla Procura Generale, p. 7.

[60] O sottoposti a procedimento amministrativo punitivo, secondo l'interpretazione data dalla Corte EDU alla luce dei criteri *Engel*, cfr. Corte EDU, *Engel e a. c. Paesi Bassi*, ricorsi n. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, 8 giugno 1976.

dei mezzi prescelti per ogni intervento pubblico nella sfera della libertà personale, intercettazioni incluse, rappresentando oggi «una colonna portante di tutto l'edificio europeo, e in particolare di quello UE»[61].

Innanzitutto, una effettiva tutela degli interessi in gioco richiede di poter effettivamente escludere forme di *surveillance* al di fuori dei casi indicati; un obiettivo tanto più importante dato l'enorme potenziale intrusivo dei nuovi strumenti informatici e che va oltre alla mera disciplina delle intercettazioni fra presenti e che non può essere lasciato solo all'evoluzione interpretativa in sede giurisprudenziale. È già stato sottolineato in dottrina come le registrazioni effettuate tramite captatori informatici, di per sé, possano anche non richiedere il contributo di soggetti terzi rispetto agli inquirenti, con la conseguenza che l'attività di *remote forensics* rischia di passare totalmente nelle mani del tecnico nominato ausiliario di polizia giudiziaria[62]. Per sopperire alla mancanza di trasparenza sulle modalità di svolgimento delle operazioni, potrebbe quindi essere opportuno promuovere l'installazione generalizzata sui dispositivi comuni (quali *smartphone*, *computer*, *tablet*) di strumenti tecnici atti a prevenire materialmente l'illecita intrusione da parte delle forze dell'ordine (e non solo). Parallelamente, protocolli chiari e pubblici dovrebbero essere stabiliti con i produttori dei dispositivi per consentire lo svolgimento delle operazioni investigative ogni qual volta ne sussistano i presupposti di legge.

Dal punto di vista procedurale, inoltre, la disciplina delle intercettazioni necessita forse di un sostanziale rafforzamento nelle sue fasi preliminari.

In particolare, poiché l'applicazione della disciplina derogatoria del d.l. 152/1991 comporta un sostanziale pregiudizio per la posizione dell'indagato e dei suoi diritti, sarebbe opportuno introdurre un controllo sulla discrezionalità del pubblico ministero nel momento della definizione della qualificazione giuridica del fatto. La delicatezza di questo passaggio è stata presa brevemente in considerazione anche dalla sentenza in oggetto, dove si richiede che la «qualificazione, pura provvisoria, del fatto come inquadrabile in un contesto di criminalità organizzata, risulti ancorato a sufficienti, sicuri e obiettivi elementi indiziari che ne sorreggano […] la corretta formulazione da parte del pubblico ministero». La necessità di un tale controllo è chiaramente volta ad evitare abusi dovuti alla raccolta di informazioni anche estremamente sensibili e il rischio della divulgazione legato a tale raccolta, per i quali – come già sottolineato dalla Corte – la sanzione successiva di inutilizzabilità non presenta garanzie sufficienti.

In tal senso, tenuto conto delle potenzialità estremamente ampie degli strumenti utilizzabili, la possibilità di procedere d'urgenza in assenza di previa autorizzazione del

---

[61] CAIANIELLO, *Il principio di proporzionalità nel procedimento penale*, in *Dir. Pen. Cont. – Riv. Trim.*, n. 3-4/2014, p. 148 ss. Per una trattazione approfondita del ruolo del principio di proporzionalità nel sistema UE, si veda anche TRIDIMAS, *The General Principles of EU Law*, Oxford EC Law Library, II ed., 2006, p. 136 ss. Cfr. anche NEGRI, Fumus commissi delicti, *La prova per le fattispecie cautelari*, Giappichelli, Torino, 2004, p. 12. Si veda anche MARLETTA, *Il principio di proporzionalità nella disciplina del mandato d'arresto europeo, tesi dottorale*, Bologna, 2013, p. 75 ss.

[62] TORRE, *Il* virus *di Stato nel diritto vivente*, cit., p. 1171.

giudice *ex* art. 267 comma 2 c.p.p. andrebbe forse riconsiderata, almeno nel caso di intercettazioni fra presenti.

Le garanzie procedurali dovrebbero infine essere rafforzate per quanto riguarda gli strumenti tecnico-informatici utilizzati per le intercettazioni, sui cui sarebbe auspicabile prevedere forme di controllo pubblico. Ciò potrebbe essere realizzato tramite la creazione di albi pubblici per gli ausiliari informatici a disposizione della Procura e tramite l'instaurazione di obblighi di relazione periodica al Parlamento o direttamente all'opinione pubblica, sulla linea di quanto già previsto in altri ordinamenti[63].

[63] Cfr. GIORDANO - VENEGONI, *La Corte Costituzionale tedesca*, cit.