La tutela della riservatezza nell'era delle nuove tecnologie: la vicenda dei captatori informatici per le intercettazioni tra presenti nei reati di terrorismo

L'utilizzo dei virus trojans nelle operazioni di intercettazioni tra presenti, a seguito della sentenza delle Sezioni unite della Corte di Cassazione (n. 26889/2016), riaccende il dibattito circa la necessità di un intervento del legislatore

Privacy Protection in the Era of New Technologies: the Case of I.T. Sensors for Telephone Wiretapping Operations Against Terrorism

As a Result of the Italian Court of Cassation Judgment (Joint Divisions, no. 26889/2016), the Use of IT Sensors in Wiretapping Operations Reignites the Debate Regarding the Necessity of Legislative Action

Caroline Peloso
Dottoranda di ricerca in Procedura penale in cotutela presso l'Università di Torino e l'Institut de sciences criminelles et de la justice dell'Università di Bordeaux

Captatori informatici, Intercettazioni tra presenti, Inviolabilità della sfera di riservatezza del singolo

IT Sensors, Wiretapping Operations, Individuals' Right to Privacy

Abstract

Gli atti di terrorismo trovano una fonte importante in un'intricata e capillare rete di informazioni diffusa tramite i sistemi informatici: il controllo e la gestione di tali flussi di comunicazioni costituisce pertanto un presupposto essenziale nella lotta al fenomeno terrorista, sia sul terreno delle indagini che all'interno del processo penale. In tale contesto, si assiste al ricorso a strumenti investigativi, come il captatore informatico, che rischiano di mettere a dura prova il diritto alla riservatezza del singolo, a causa della loro forte potenza invasiva. Buona parte dei Paesi europei si sono pertanto trovati a confrontarsi con la sfida che vede contrapposte l'efficacia di certe tecnologie e la tradizionale salvaguardia delle libertà fondamentali, patrimonio insuperabile della cultura giuridica occidentale. L'Italia non è esente da tale sfida. In questo breve contributo si cercherà di riscoprire, soprattutto alla luce di una recente sentenza delle Sezioni Unite della Corte di cassazione, la situazione nazionale, avendo riguardo anche alle soluzioni adottate in alcuni altri Paesi dell'Unione europea.

Acts of terrorism use the intricate and widespread network of information communicated through computer systems as an important source: the control and management of this flow of communication is, therefore, an essential prerequisite in the fight against the terroristic phenomenon and in the field of investigations within the criminal law process. In this context, we see the use of investigative tools such as IT sensors risk placing a considerable strain on an individual's right to privacy, due to their markedly invasive power. Most European countries have, therefore, found themselves coping with the challenge of balancing between the effectiveness of certain technologies and the traditional protection of fundamental freedoms; an unequalled heritage of Western legal culture. Italy is not exempt from this challenge. In this brief article, I seek to re-evaluate, especially in light of a recent judgment from the Joint Divisions of the Court of Cassation, the national situation while also taking into consideration the solutions adopted in other European Union countries.

Sommario

1. La nozione di captatore informatico e le sue implicazioni tecnico-giuridiche.

La problematica questione dell'uso occulto dei captatori informatici - anche detti *trojan* o *spyware* - per eseguire operazioni di intercettazione su supporti informatici altrui, è questione quanto mai attuale[1]. Il ricorso a tali strumenti informatici, dal carattere di spiccata invadenza, pone infatti un serio e preoccupante[2] interrogativo circa la legittimità del loro utilizzo rispetto alla sfera di riservatezza del singolo: quest'ultima, infatti, considerata espressione diretta di un nucleo di diritti fondamentali tutelati a livello costituzionale da una doppia riserva, di legge e di giurisdizione, e a livello sovranazionale, rischia di subire un'importante compressione a seguito dell'impiego dei *trojans* per intercettazioni di comunicazioni tra presenti in assenza di un quadro normativo di riferimento[3]. Si tratta di un problema che – sebbene risalente - rischia di aggravarsi ulteriormente nel generale clima di insicurezza determinato da fatti di terrorismo, e che non pare certo contrastato dall'atteggiamento mostrato dalla giurisprudenza - come, ad esempio nella recente pronuncia delle Sezioni Unite n. 26889/2016[4] - che, anzi, sembra voler piuttosto ricercare una soluzione rapida, volta a garantire un senso di sicurezza contro crimini odiosi come quelli di matrice terroristica, dimenticando talvolta il necessario bilanciamento con le garanzie costituzionali assicurate all'indagato il quale, per primo, è chiamato a pagarne le conseguenze.

In particolare, l'uso del virus informatico per compiere operazioni di intercettazione nell'ambito della criminalità organizzata, anche di stampo terroristico, costituisce - secondo una definizione pienamente calzante offerta dalla Sesta Sezione della Corte di Cassazione nell'ordinanza di rimessione alle Sezioni Unite - uno strumento di "*formidabile invadenza*" che conduce gli operatori del diritto ad interrogarsi sulla natura delle intercettazioni operate tramite captatore informatico, nonché sull'esigenza di un intervento legislativo che regoli modalità, limiti e garanzie con cui tali operazioni possano trovare la loro collocazione nel nostro ordinamento, in uno sforzo di bilanciamento con i principi costituzionali e sovranazionali[5].

Il captatore informatico *o trojan horse* o *spyware* – come si voglia chiamarlo - è un programma che si installa in maniera occulta sugli apparecchi elettronici che si intendono moni-

[1] In materia: M. Torre, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondament*ali, in *Dir. Pen. Proc.*, 2015, 9, 1163; S. De Flammineis, *Le intercettazioni telematiche*, *Dir. Pen. Proc.*, 2013, 8, 988; M.T. Abbagnale, *In tema di captatore informatico,* in *Arch. Pen*. n.2/2016; A. Testaguzza, *Exitus acta probat "Trojan" di Stato: la composizione di un conflitto*, in *Arch. Pen.*, n.2/2016.

[2] Preoccupazione per il vuoto normativo è stata espressa recentemente proprio dai docenti di Diritto processuale penale dell'Università di Torino in un appello al legislatore, sottoscritto da altri numerosi docenti italiani della materia: *Necessaria una disciplina legislativa in materia di captatori informatici (c.d. trojan): un appello al legislatore da parte di numerosi docenti di diritto italiani*, in *Dir. pen. cont.*, 7 ottobre 2016; stessa preoccupazione è stata manifestate dall'Unione delle Camere penali italiane in un comunicato relativo all'astensione nazionale dei penalisti il 24-26 maggio 2016.

[3] Per un quadro dei profili costituzionali in materia di intercettazioni tra gli altri: cfr. F. Caprioli, *Colloqui riservati e prova penale*, Giappichelli, 2000; C. Marinelli, *Intercettazioni processuali e nuovi mezzi di ricerca della prova*, Giappichelli, 2007; L. Filippi, *L'intercettazione di comunicazioni,* Giuffré, 2007; A. Camon, *Le intercettazioni nel processo penale*, Giuffré, 1996; e più in generale sulla portata degli artt. 14 e 15 della Carta Costituzionale si rimanda a p. caretti, *I diritti fondamentali*, Giappichelli, 2011, 293*: "il diritto alla riservatezza viene definito come il diritto a mantenere riservato, salva espressa dichiarazione di volontà in senso contrario, quegli aspetti della propria vita privata, che attengono a fatti personalissimi che proprio per questo il soggetto ha il diritto di sottrarre alla conoscibilità dei terzi*".

[4] Per un commento alla pronuncia delle Sezioni Unite: G. Lasagni, *L'uso di captatori informatici (trojans) nelle intercettazioni "fra presenti"*, commento a Cass. Pen. Sez. un. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889, Pres. Canzio. Rel. Romis, Imp. Scusato, in *Dir. pen.* cont, 7 ottobre 2016.

[5] Più specificamente sul tema del Digital forensics, ovvero la scienza che si occupa dell'identificazione, conservazione, analisi e documentazione dei dati estrapolati da dispositivi informatici (computer, server, smartphone, network, cloud, social network) al fine di produrre elementi di prova in procedimenti civili e penali e i rapporti con i principi dell'ordinamento: A. Testaguzza, *Digital forensics, informatica giuridica e processo penale*, Cedam, 2015; F. Ruggieri, *Profili processuali nelle investigazioni informatiche,* in *Il diritto penale dell'informatica nell'epoca di internet,* (a cura di) L. Picotti, Cedam, 2004, 153; P. Ferri, *Computer forensics* in *Dig. Disc. Pen*., 2015, 95; s. aterno , *Digital forensics*, in *Dig. Disc. Pen*, 2015, 217.

torare (*personal computers, tablets, smartphones)* grazie a una cosiddetta "inoculazione" operata fisicamente, se il dispositivo è lasciato incustodito, o da remoto (tramite l'invio di allegati a messaggi di posta elettronica, aggiornamenti di applicazioni, messaggistica ecc., da cui l'etimologia di *trojan*, che rimanda chiaramente al famoso inganno teso ai Troiani). La straordinaria forza invasiva del captatore pone molteplici problemi che solo in parte coincidono con l'istituto delle intercettazioni telefoniche o tra presenti *tout court*[6] e con le intercettazioni di comunicazioni di cui agli artt. 266 c.p.p. e seguenti, unico istituto su cui le Sezioni Unite qui citate affrontano il problema dell'uso dei captatori informatici, le quali si concentrano in particolare sulla questione inerente il luogo in cui l'intercettazione con il captatore deve avvenire[7].

Infatti, come ebbero modo di ricordare le Sezioni Unite della Corte di cassazione nella decisione n. 36747 del 2003 c.d. *Torcasio*[8] , con la nozione di intercettazione di comunicazioni si intende "*qualsiasi captazione occulta e in tempo reale di una conversazione tra due persone - le quali intendono escluderne gli altri con modalità atte allo scopo - da parte di altri soggetti mediante strumenti tecnici invasivi ed insidiosi capaci di superare le cautele elementari che dovrebbero garantire libertà e sicurezza del colloquio*". Tuttavia è evidente che quando ci si addentra nel tema dell'uso del captatore informatico si fa riferimento ad una molteplicità di operazioni intrusive differenti, attuate sul dispositivo controllato, come la cattura di quanto viene visualizzato sullo schermo o digitato sulla tastiera, la registrazione di suoni o immagini attraverso il microfono o la videocamera, il salvataggio e la copia dei file presenti sul dispositivo, che consentono di entrare nel pieno possesso del dispositivo elettronico e che non possono certo esser fatte rientrare nell'istituto di cui all'art. 266 c.p.p. , ma che necessiterebbero un rinvio ad altri mezzi di ricerca della prova quali le perquisizioni, le ispezioni e il sequestro di sistemi o supporti informatici[9].

Orbene, essendo il tema delle intercettazioni telefoniche e di comunicazioni strettamente legato ai principi di inviolabilità del domicilio, di cui all'art. 14 Cost, e di libertà e segretezza nelle comunicazioni, di cui all'art. 15 Cost., garantititi da una riserva di legge e di giurisdizione, ne deriva che un utilizzo dei captatori informatici che avvenga in assenza di un quadro normativo di riferimento - che indichi le ragioni giustificatrici del ricorso a strumenti di tale invasività e ne preveda modalità e limiti del loro utilizzo - rischia di porsi in aperta violazione con i citati principi, diretti a garantire l'immunità dello spazio privato del singolo contro ogni ingerenza dei poteri pubblici[10]. Non solo. La intensa capacità intrusiva dei nuovi mezzi investigativi, a fronte del diritto alla riservatezza del singolo, impone l'allargamento del quadro di tutela agli artt. 2 e 3 Cost e all'inviolabilità della libertà personale di cui all'art. 13 Cost.[11],

[6] Sul concetto di intercettazione come operazione occulta di presa di conoscenza del contenuto di una conversazione tra presenti o di una comunicazione tra assenti, anche informatica o telematica, di carattere riservato, effettuata a scopo investigativo dagli organi inquirenti sotto il controllo giurisdizionale preventivo o successivo, ed eseguita mediante strumenti tecnici idonei alla captazione e alla registrazione in tempo reato del dato comunicativo: cfr. C. Marinelli, op. cit., p. 6; P.F. Bruno, voce *Intercettazioni di comunicazioni o conversazioni*, in *Dig. Pen.,* VII, 1993, p. 178; L. Filippi, voce *Intercettazioni telefoniche (diritto processuale penale*), in *Enc. Dir*., vol. VI, Milano, 2001 p. 565; G. Illuminati, *La disciplina processuale delle intercettazioni,* Giuffré, Milano, 1983.

[7] La Corte infatti nella sentenza Cass. 26889/2016, Scurato, (p. 11) delimita l'ambito del suo intervento, così come delineato dall'ordinanza di rimessione, alle sole intercettazioni "ambientali"e pertanto si riferisce agli istituti disciplinati agli artt. 266 ss. del Codice di procedura penale.

[8] Cass. Sez. Un. , 28 maggio 2003, dep. 24 settembre 2003, n. 36747, Pres. Marvulli,, Rel. Milo, Imp. Torcasio, in *Cass. Pen*. 2004, p. 2094.

[9] La legge del 18 marzo 2008 n. 48 di Ratifica della convenzione del Consiglio d'Europa sulla criminalità informatica (Budapest, 23 novembre 2001) ha ricondotto ai mezzi tipici di ricerca della prova le perquisizioni, le ispezioni e i sequestri di supporti informatici.

[10] F. Caprioli, *Intercettazioni illecite, intercettazioni illegali, intercettazioni illegittime,* in Aa.Vv., *Le intercettazioni di conversazioni e comunicazioni: un problema cruciale per la civiltà e l'efficienza del processo e per le garanzie dei diritti: atti del Convegno,* Milano, 5-7 ottobre 2007, Giuffré, Milano, 2009, 137: *il paradigma di intercettazione legittima/illegittima si riferisce alla loro conformità o difformità rispetto al modello normativo risultante dalla normativa processuale e alla conseguente utilizzabilità/inutilizzabilità probatoria dei risultati [..] l'espressione liceità/illiceità si riferisce alla conformità alla fattispecie di natura sostanziale il cui perfezionarsi determina conseguenze sanzionatorie per l'agente [..] intercettazione illegali comprende le intercettazioni illegittime e illecite ed indica la loro contrarietà alla legge, processuale o sostanziale*"; g. spangher, *Le criticità della disciplina delle intercettazioni telefoniche*, in *Dir. Pen. Processo*, 2016, 7, 921.

[11] A. Gaito – S. Furfaro, *Le nuove intercettazioni "ambulanti": tra diritto dei cittadini alla riservatezza ed esigenze di sicurezza per la collettività*, in *Arch. Pen*., 2/2012, 11 ricordano come la Corte Costituzionale con decisione n.38/1973 abbia ricondotto il diritto alla riservatezza tra i diritti inviolabili costituzionalmente garantiti; d'altronde anche P. Caretti, *op. cit.* p. 292 ricorda come il diritto alla riservatezza, non menzionato espressamente dal testo costituzionale , non è limitato alla sola tutela del domicilio e della corrispondenza, ma rappresenta un caso di interpretazione estensiva, grazie all'intervento dei giudici comuni (in particolare della Corte di cassazione) e della Corte Costituzionale, che hanno colto nell'art. 2 – inteso come clausola aperta – e nell'art. 3 – che allude alla tutela della dignità sociale – i punti a cui ancorare il diritto alla riservatezza. Tale legame è effettuato anche con riferimento all'art. 13 Cost. laddove la libertà personale è intesa come "libertà-situazione" ovvero situazione legata alla posizione della persona rispetto ai poteri dei pubblici poteri e dei privati.

oltre che ai principi sovranazionali, tra cui assume particolare importanza l'art. 8 Cedu[12], che riconosce ad ogni persona il diritto al rispetto della sua vita privata e familiare, del domicilio, e della corrispondenza.

E' innegabile che, nei reati di terrorismo, l'acquisizione delle informazioni mediante intercettazione, anche informatica, appare fondamentale: è proprio infatti attraverso il ricorso a comunicazioni e dati (scambio di foto, video, messaggi vocali etc..), tramite dispositivi elettronici che si attua il reclutamento, la diffusione di messaggi e l'indicazione delle modalità operative della rete e dell'azione terroristica; il carattere occulto e clandestino che connatura l'intercettazione è infatti elemento essenziale per poter scoprire ed acquisire elementi che, nel quadro delle indagini, consentano di prevenire, anticipandoli, eventuali gravi atti di violenza contro le persone e contro la sicurezza pubblica[13] e, per altro verso, costituiscano, ai fini processuali, elementi di prova. Si tratta quindi di un'arma a doppio taglio: gli strumenti *de quibus* sono, senza ombra di dubbio, non solo utili, ma necessari, nel contesto attuale in cui le organizzazioni criminali terroristiche presentano una capacità tecnologica anch'essa molto elevata e sofisticata per sfuggire alle indagini di polizia, ma allo stesso tempo non possono essere autorizzati se non all'interno di un preciso quadro legislativo di riferimento – al momento non esistente, pena il rischio di sacrificare in nome del bisogno di sicurezza, valori imprescindibili di libertà dell'individuo profondamente radicati nella nostra storia nazionale e nel patrimonio comune europeo.

2. Il tema dei captatori informatici nella prassi italiana.

Occorre fare un breve *excursus* della comparsa e dello sviluppo del captatore informatico nella prassi italiana. Una delle prime pronunce in cui la giurisprudenza di legittimità ha affrontato il tema è stata la sentenza n. 16556 del 14 ottobre 2009[14], in cui si dibatteva circa l'utilizzo da parte della polizia di un captatore informatico per acquisire e copiare *files* contenuti all'interno di un *personal computer* in uso agli indagati; tale operazione era stata autorizzata dal P.M. tramite decreto di acquisizione di atti *ex* art. 234 c.p.p. che i giudici avevano ritenuta legittima, qualificandola come acquisizione di dati e non come "flusso di comunicazioni", riconducendo i dati ottenuti alla categoria delle "*prove atipiche*" di cui all'art. 189 c.p.p. ed escludendo l'applicabilità degli artt. 266 e ss. c.p.p.[15]. Successivamente, intervenne in materia di captatori la decisione della Corte di Cassazione n. 254865/2010[16] relativa a una ipotesi di associazione di stampo massonico P4, in cui il Gip, richiesto di autorizzare delle operazioni con captatori informatici, aveva ritenuto sufficiente l'acquisizione dei dati tramite il ricorso al provvedimento di cui all'art. 234 c.p.p. - non qualificando (come già accaduto nel caso precedente) questa attività come intercettazione - senza necessità di autorizzazione; anche in tal caso i giudici del Supremo Collegio ritennero tale qualificazione corretta, decisione che fece preconizzare il rischio di un'insidiosa violazione dei diritti fondamentali sottesa alla qualificazione di tali mezzi di prova, particolarmente invadenti come i *trojan*s, nella categoria delle prove atipiche, sottraendoli alla più rigorosa disciplina delle intercettazioni predisposta dagli

[12] L'art 8 CEDU riconosce ad ogni persona il diritto al rispetto della sua vita privata e familiare, del domicilio e della corrispondenza, in tal senso si devono escludere tutte le interferenze nella sfera privata dell'autorità pubblica salvo che esse siano previste da una legge, siano necessarie in una società democratica e siano necessarie per la sicurezza nazionale. Sull'art. 8 CEDU, tra gli altri: D. DONATI, *Il diritto alla riservatezza e il diritto alle libertà di espressione. Le intercettazioni di conversazioni o comunicazioni*, in *L'integrazione attraverso i diritti*, *L'Europa dopo Lisbona, Atti del I Workshop in Diritto dell'Unione europea e internazionale, Venezia Palazzo Ducale, 26-27 marzo 2010*, (a cura di) E. Falletti, V. piccone,Aracne, Roma, 2010, 453; C. Marinelli, op.cit, p. 63; L. Filippi, op. ct, 43.

[13] Sulla natura clandestina e occulta che deve avere l'intercettazione: G. ILLUMINATI, *La disciplina processuale delle intercettazioni*, op. cit, pag. 34: "*poiché oggetto dell'intercettazione sono le comunicazioni o conversazioni riservate, è necessario che l'operazione avvenga all'insaputa degli interessati. In caso contrario verrebbe meno la principale utilità dello strumento, basata appunto sulla possibilità di scoprire elementi di prova che verosimilmente gli interlocutori non apporterebbero al processo di propria volontà*".

[14] Cass., Sez. V, 14 ottobre 2009, *Virruso* in Mass. Uff. n. 246955; La Corte concludeva così" " *è legittimo il decreto del pubblico ministero di acquisizione in copia, attraverso l'installazione di un captatore informatico, della documentazione informatica memorizzata nel personal computer in uso all'imputato e installato presso un ufficio pubblico qualora il provvedimento abbia riguardato l'estrapolazione di dati, non aventi ad oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del personal computer o che in futuro sarebbero stati memorizzati*".

[15] La Corte di Cassazione escludeva anche qualsiasi violazione dell'art. 14 della Costituzione perché l'apparecchio monitorato si trovava nei locali di un ufficio pubblico comunale e non nel domicilio o in luogo di privata dimora, né tali documenti potevano rientrare nel concetto di corrispondenza o di altre forme di comunicazione di cui all'art. 15 Costituzione posto che si trattava di testo da stampare su supporto cartaceo e da consegnare al suo destinatario".

[16] Cass. Sez. VI, 27 novembre 2012, *Bisignani*, in *Mass. Uff.* n. 254865.

artt. 266 e seguenti del Codice di procedura penale.

Nel 2015, invece, con la sentenza n. 27100/2015[17], i giudici cambiarono decisamente rotta. Il caso aveva ad oggetto il ricorso per cassazione contro l'ordinanza del Tribunale del riesame di Catania che confermava una misura cautelare proprio sulla base di intercettazioni effettuate tramite un virus informatico: in particolare, la difesa lamentava una violazione degli artt. 14 e 15 Cost. e dell'art. 8 Cedu, affermando come le intercettazioni non fossero state oggetto di alcuna restrizione temporale o spaziale. La Corte qualificava, questa volta, i dati acquisiti come rientranti nel novero delle intercettazioni ambientali – e come tali sottoposte alla disciplina di cui all'art. 266, 2° comma c.p.p. - dichiarandone la radicale inutilizzabilità, dal momento che le intercettazioni, come chiariva la sentenza, devono avvenire in luoghi identificati sin dall'inizio nel decreto del G.i.p, non potendo essere considerata in alcun modo legittima un'intercettazione effettuata in un qualsiasi luogo in cui il soggetto porti con sé l'apparecchio elettronico[18]. Nella citata decisione, infatti i giudici della Sesta Sezione sostenevano che una lettura compatibile con l'art. 15 della Costituzione del 2° comma dell'art. 266 c.p.p richiedesse la previa individuazione *ab origine* del luogo in cui la captazione debba avvenire: infatti la precisazione del luogo non era considerata una semplice modalità operativa dell'intercettazione, ma una peculiare tecnica di captazione e, come tale, dunque, costituiva una condizione fondamentale della legittimità delle operazioni intercettive stesse. A conferma di tale interpretazione i giudici richiamavano, infatti, i precedenti giurisprudenziali che ammettevano la variazione del luogo di captazione solo quando "*rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata*"[19], così negando un'operatività ad ampio raggio dell'intercettazione tra presenti.

Un caso analogo a quello oggetto della decisione n. 2700/2015 era all'origine della Sentenza delle Sezioni Unite n. 26889/2016 : il difensore dell'imputato, infatti, aveva promosso un ricorso in cassazione contro l'ordinanza del Tribunale del riesame di Palermo che in data 8 gennaio 2016, ritenendo sussistenti i gravi indizi di colpevolezza sulla base di indizi emersi durante le operazioni di intercettazioni ambientali e delle dichiarazione di due collaboratori di giustizia, applicava la misura della custodia cautelare in carcere. Le doglianze della difesa avevano ad oggetto la violazione dell'art. 14 Cost. nonché degli artt. 15 Cost. e 8 della Convenzione europea, in quanto l'autorizzazione ad effettuare le intercettazioni indicava come luogo di captazione " *quello ove fosse ubicato in quel momento l'apparecchio portatile*". Il difensore si richiamava dunque alla precedente 'giurisprudenza *Musumeci*' - che aveva fatto del "luogo" di captazione un criterio fondamentale di legittimità delle operazioni intercettive - chiedendo che fosse accertata l'illegittimità e l'inutilizzabilità delle conversazioni captate in luoghi non previamente identificati.

La Sesta Sezione della Corte di Cassazione, tuttavia, si mostrava critica verso le conclusioni della richiamata decisione soprattutto nella parte in cui - non tenendo per nulla in conto la specificità dell'intercettazione tra presenti rispetto alle captazioni telefoniche - poneva come criterio fondante la legittimità dell'intercettazione mediante captatore informatico la previa identificazione del luogo[20] ; inoltre si sottolineava come, allora, i giudici avessero omesso di prendere in considerazione la disciplina derogatoria di cui all'art. 13 d.l. 13 maggio 1991 n. 152 (convertito con modificazioni dalla legge 203/1991), prevista per i reati di criminalità organizzata e terrorista, rispetto a cui l'indicazione locale è del tutto irrilevante, posto che i luoghi di privata dimora non sono, nell'ambito di quei procedimenti, soggetti ad alcuna disciplina particolare rispetto agli altri luoghi. Pertanto, alla luce di tali considerazioni, la Sesta Sezione rimetteva la questione alle Sezioni Unite, con ordinanza del 10 marzo 2016, formulando il seguente quesito : "*se anche nei luoghi di privata dimora ex. art. 614 c.p. non singolarmente in-*

[17] Cass. Sez. VI, 26 maggio 2015, *Musumeci*, in *Guida dir*., n. 41, 2015, 83.

[18] Punto 2 dei motivi della decisione: "[…] *'intercettazione telematica, tramite agente intrusore (virus informatico), che consenta l'apprensione delle conversazioni tra presenti mediante l'attivazione, attraverso il virus informatico, del microfono di un apparecchio telefonico smartphone, non è giuridicamente ammissibile. Nel caso di specie, la tecnica utilizzata consente, attraverso l'attivazione del microfono del telefono cellulare, la captazione di comunicazioni in qualsiasi luogo si rechi il soggetto, portando con sè l'apparecchio: ciò che, come poc'anzi evidenziato , non è giuridicamente ammissibile. Non si tratta pertanto, come erroneamente ritenuto dal Tribunale, di una semplice modalità attuativa del mezzo di ricerca della prova, costituito dalle intercettazioni. Si tratta invece di una tecnica di captazione che presenta delle specifiche peculiarità e che aggiunge un quid pluris, rispetto alle ordinarie potenzialità dell'intercettazione, costituito, per l'appunto, dalla possibilità di captare conversazioni tra presenti non solo in una pluralità di luoghi , a seconda degli spostamenti del soggetto, ma – ciò che costituisce il fulcro problematico della questione– senza limitazione di luogo. Ciò è inibito, prima ancora che dalla normativa codicistica, dal precetto costituzionale di cui all'art. 15 Cost...[..]'*".

[19] In tal senso Cass. Sez. IV, 11 dicembre 2007, n. 15396 ; Cass. Sez. II, 15 dicembre 2010, n.4178.

[20] la Sezione rimettente sottolineava come " *la pretesa di indicare con precisione e anticipatamente i luoghi interessati dall'attività di captazione fosse incompatibile con questo tipo di intercettazioni che, per ragioni tecniche, in quanto collegata al dispositivo elettronico sia smartphone o tablet o pc portatile, prescinde dal riferimento al luogo*".

dividuati 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 informatico in dispositivi elettronici portatili".

3. L'iter argomentativo seguito dalle Sezioni Unite della Corte di Cassazione nel caso c.d. *Scurato*.

La Corte, al fine di rispondere al quesito sottopostole, si basava su due argomentazioni assenti nella giurisprudenza del 2700/2015; *in primis* valutava la legittimità delle intercettazioni mediante captatore operando un distinguo, che la giurisprudenza *Musumeci* aveva tralasciato, tra i procedimenti per i reati soggetti alla disciplina ordinaria di cui agli artt. 266 ss c.p.p., e le indagini aventi ad oggetto criminalità organizzata anche terroristica, cui si applica la disciplina derogatoria dell'art. 13 d.l. 152 del 1991, la quale ammette che "*l'autorizzazione a disporre le operazioni di cui all'art. 266 c.p.p. è data, in deroga a quanto prevede l'art. 267, quando l'intercettazione è necessaria per lo svolgimento di indagini in relazione a delitti di criminalità organizzata in ordine al quale sussistono sufficienti indizi* "[…] Ed in particolare " *quando si tratta di intercettazioni di comunicazioni tra presenti disposta in un procedimento per delitti di criminalità organizzata e che avvenga nei luoghi di cui all'art. 614 c.p. – quindi privata dimora - l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa*".

La Corte operava tale distinzione sotto il profilo di come la diversa disciplina applicabile incida sulla necessità di previa indicazione del luogo in cui l'intercettazione deve avvenire, seppur limitatamente ai luoghi di privata dimora. Inoltre, la Suprema Corte, sottolineava come la sentenza n. 2700/2015, oltre a presentare una lacuna importante nel mancato riferimento alla disciplina derogatoria, faceva riferimento alla nozione di intercettazione *ambientale*, che costituisce in realtà una nozione priva di riscontro normativo, sia nella disciplina ordinaria di cui all'art. 266, 2° comma c.p.p., sia in quella derogatoria di cui all'art. 13 d.l. 152/91. Infatti il termine "ambientale" costituisce piuttosto un'espressione diffusasi nella prassi per indicare che le "cimici" o microspie - all'epoca in cui i *trojan virus* erano ancora ben lungi dall'essere immaginati - sarebbero state installate in luoghi chiusi riconducibili a determinati ambienti; ciò significa che la distinzione operata dai giudici nella sentenza 2700/2015 basata sulla dicotomia tra "*intercettazioni tra presenti in ambienti predeterminati*" e "*intercettazioni tra presenti in ambienti non previamente determinati*" è priva di qualsiasi aggancio normativo dal momento che ne la legge ne la giurisprudenza richiedono la predeterminazione del luogo come condizione di legittimità della captazione[21]. L'unica differenza rilevante infatti è quella contenuta nel solo 2° comma dell'art. 266 c.p.p tra "*intercettazioni tra presenti che avvengano in luoghi diversi da quelli di cui all'art. 614 c.p.p. ovvero di privata dimora*" - rispetto a cui non è richiesta alcuna condizione particolare - e le "*intercettazioni tra presenti che avvengano in luoghi di privata dimora*": in quest'ultimo caso, l'intercettazione potrà aver luogo solo quando vi è un fondato motivo di ritenere che ivi si stia svolgendo un'attività criminosa. E' dunque solo con riferimento a quest'ultima categoria che la legge e la giurisprudenza, dando rilievo alla natura itinerante del captatore, richiedono la previa individuazione del luogo allorquando si tratta di privata dimora.

Infatti l'intercettazione operata a mezzo virus informatico in luoghi di privata dimora nel caso di procedimenti per reati ordinari – in quanto tale sottoposta alla disciplina ordinaria del Codice di procedura penale - deve sempre essere considerata come illegittima, poiché il giudice non può prevedere i luoghi in cui tale apparecchio sarà spostato e introdotto, verificando all'uopo, come prevede la legge, che ivi vi sia in corso un'attività criminosa; e, in ogni caso, anche qualora tale previsione fosse possibile, essa comunque si sottrarrebbe a qualsiasi controllo al momento dell'autorizzazione sicché sarebbe comunque, per riprendere l'espressione

[21] Orientamento supportato anche dalla giurisprudenza europea che, come sottolinea la Memoria della procura generale presso la Corte di Cassazione per la Camera di consiglio delle Sezioni Unite del 28 aprile 2016, in *Dir. pen. cont.*, che non annovera il luogo tra gli elementi necessari, prevedendo che il decreto autorizzativo deve menzionare: la tipologia delle comunicazioni oggetto dell'intercettazione, i reati che giustificano il ricorso a tale mezzo, l'attribuzione ad un organo indipendente della competenza ad autorizzate le intercettazioni, le categorie di persone interessate, i limiti di durata, la procedura da usare e i casi di distruzione del materia; cfr. Corte Edu , Vetter c. Francia, 31 maggio 2005; Corte Edu, Kennedy c. Regno Unito, 18 maggio 2010.

dei giudici, "*un'autorizzazione disposta al buio*". Ne deriva pertanto che, autorizzando l'uso dei captatori informatici nei procedimenti sottoposti a disciplina ordinaria, vi sarebbe il rischio di operare una pluralità di intercettazioni violando i limiti imposti dal codice di rito, dalle norme costituzionali e sovranazionali. Ne consegue che, nei procedimenti per reati ordinari, l'uso dei captatori non potrebbe mai essere considerato legittimo nell'ambito delle operazioni intercettive, alla luce dell'attuale testo dell'art. 266, 2° comma c.p.p.

Al contrario, per quanto riguarda i procedimenti relativi ai delitti di criminalità organizzata e terrorismo, le differenza tra le due categorie viene definitivamente meno in virtù dell'indifferenza per il criterio dello svolgimento dell'attività criminosa.

La Corte dunque traeva una prima conseguenza ovvero : se la norma derogatoria consente l'intercettazione tra presenti, anche qualora non vi sia motivo di ritenere che nel luogo di privata dimora sia in corso un'attività criminosa, essa traduce un espresso bilanciamento operato dal legislatore, volto a rendere più facile l'operatività del mezzo investigativo, a fronte di reati di maggiore gravità e pericolosità. In secondo luogo, si deduce che, se nelle intercettazioni ambientali relative a procedimenti di criminalità organizzata la scelta del legislatore è quella di ritenere irrilevanti le caratteristiche del luogo in cui la captazione avviene, a maggior ragione lo stesso deve avvenire per quelle intercettazioni che si avvalgono di un mezzo, quale il *trojan*, che per sua natura, costituisce uno strumento captativo *itinerante,* rispetto al quale è del tutto impensabile individuare preventivamente i luoghi in cui la captazione sarà effettuata. Tuttavia, ciò non significa che il giudice non sia tenuto, anche nell'ipotesi derogatoria, a motivare in merito alla necessità di eseguire l'accertamento in determinati luoghi, posto che egli deve comunque argomentare il legame di utilità nel disporre l'intercettazione in un certo ambiente, non potendo certo ammettersi una intercettazione *"a tappeto*".

Le Sezioni Unite dunque, con particolare disinvoltura, autorizzavano l'uso dei captatori informatici limitatamente ai procedimenti di criminalità organizzata e terrorismo, forse non cogliendo l'insita pericolosità di tali mezzi investigativi seppur nell'ambito di procedimenti per reati particolarmente gravi, così riconfermando la necessità di un intervento chiarificatore del legislatore in una materia così delicata.

La sentenza giunge ad operare un'equivalenza – contestabile - tra le operazioni di intercettazioni in procedimenti per criminalità organizzata e terrorismo effettuate con i mezzi tradizionali - quali microspie o cimici - con quelle operate attraverso il *trojan virus,* affermando che il legislatore, dettando la norma derogatrice, ossia l'art. 13 dl. 152/1991, ha inteso fornire una "*precisa e significativa indicazione [circa il bilanciamento degli interessi in gioco] – pur in un contesto temporale in cui la tecnologia non aveva ancora raggiunto l'attuale livello di efficacia e di capacità intrusiva*"[22].

Ora, appare difficile pensare che una norma, senza dubbio espressione di un bilanciamento di valori, ma scritta più di due decenni fa, possa essere considerata ancora oggi lo specchio di un apprezzamento veramente attuale tra i rischi creati per la tutela della *privacy* dell'individuo da strumenti tecnologici (oggi di certo più avanzati rispetto alla fine degli anni '80 del secolo scorso) e l'interesse al perseguimento di gravi crimini per la sicurezza comune; assimilare le due modalità intercettive – "tradizionale e tecnologica" - sembra tradire un palese sbilanciamento a scapito delle garanzie dell'individuo. Peraltro, tale capacità intrusiva deve intendersi non solo sotto il profilo dell'ampio campione di informazioni che può rastrellare - chiaramente incomparabile rispetto ad una microspia - ma deve essere valutato anche sotto il profilo della sua tecnicità, sicché esso si presenta come uno strumento che richiede una competenza da "*addetto ai lavori*" per coloro che sono chiamati a gestirne limiti e modalità operative.

Ora, sul problema inerente le particolarità tecniche del captatore, giova ricordare che le indicazioni di rango europeo contenute nella Direttiva n.680/2016 in materia di dati personali vanno nel senso di optare per la c.d. "*neutralità tecnica*", secondo cui "*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*"[23]; pertanto il legislatore non dovrebbe soffermarsi sulla disciplina dei singoli strumenti informatici – sempre potenzialmente in evoluzione e dunque suscettibili di creare un vuoto di tutela in caso di mancato tempestivo

[22] pag. 20 e seguenti: "*Proprio in forza ed all'esito dell'accurato contemperamento di valori ed interessi, operato dal legislatore nell'introdurre il D.l. 152/1991 art. 13, l'eventualità di intercettazioni domiciliari, in conseguenza della mobilità del dispositivo sede del captatore, non può ritenersi in contrasto con la normativa vigente e nemmeno con i principi costituzionali posti a tutela della segretezza delle comunicazioni, del domicilio e della riservatezza, tenuto altresì conto di quanto già si è avuto modo di osservare in precedenza*".

[23] Sul punto G. Lasagni, op. cit. pag. 11 ss.

intervento legislativo – ma dovrebbe piuttosto identificare le garanzie fondamentali che devono sempre essere garantite all'indagato indifferentemente dallo strumento impiegato[24]. A tali considerazioni, assolutamente corrette in un impianto garantista , si obietta peraltro che - se è vero che la neutralità tecnica permette di assicurare uno standard di garanzie minime agli indagati, qualunque sia il tipo di strumentazione tecnica in uso all'autorità giudiziaria - sarebbe comunque auspicabile che l'intervento del legislatore, quando mai ci sarà, si mostri particolarmente aggiornato a questi nuovi tipi di strumenti tecnici, in maniera da poter offrire lumi anche sugli aspetti più tecnici. Infatti, nell'ambito dei captatori informatici e, più in generale, delle nuove tecnologie, la tutela effettiva delle garanzie fondamentali sarà fortemente legata alla specificità tecnica del mezzo, sicché non sarà possibile prescindere da un intervento legislativo quanto più preciso. Ciò implica infatti che il legislatore dovrebbe integrare dei criteri di *digital forensic*[25] alla disciplina normativa e non limitarsi ad un generico tentativo di far rientrare il mezzo investigativo in categorie ormai obsolete[26].

4. L'impiego da parte dei giudici della Suprema Corte di una definizione estesa della nozione di *criminalità organizzata*.

Altro punto interessante da rilevare con riferimento alla decisioni delle Sezioni Unite riguarda la costatazione che, per applicare il principio fatto proprio dalla Cassazione, risulterà fondamentale che il fatto rientri nella nozione di criminalità organizzata, discendendo da tale qualificazione la legittimità o meno dell'uso dei captatori[27]. Tuttavia, anche sotto il profilo del concetto di criminalità organizzata con finalità di terrorismo, non avendo il legislatore fornito una definizione precisa delle condotte che vi rientrano, bisogna rimettersi ad un generico rinvio all'art. 51 *comma 3 bis* e *3 quater* c.p.p. "*nonché a tutti quei reati facenti comunque capo ad un'associazione a delinquere ex art. 416 c.p. aventi ad oggetto attività criminose eterogenee purché realizzate da una pluralità di soggetti, i quali abbiano costituito un apposito apparato organizzativo organizzativo*". La legittimità o meno dell'uso dei captatori informatici sarebbe dunque rimessa all'esito della qualificazione del fatto effettuata dal pubblico ministero, ma sul contenuto della definizione stessa di criminalità organizzata il legislatore dovrebbe intervenire attraverso una disciplina più precisa, ad esempio immaginando che l'utilizzo del captatore informatico possa essere esteso a reati non propriamente associativi, ma comunque di rilevante gravità. Si pensi, ad esempio, al fenomeno dei c.d. "*lupi solitari*", ossia persone che svolgono attività di auto-addestramento e incitamento al terrorismo, senza necessariamente appoggiarsi a una rete più vasta o tentando di entrarvi in contatto. *A contrario,* si potrebbe immaginare di escludere il loro utilizzo con riferimento a determinate fattispecie di minore gravità.

A sottolineare il vuoto normativo interno, si ricordi che la Corte di Strasburgo, per considerare rispettato l'art. 8 della Convenzione europea esige, in materia di intercettazioni, la sussistenza di tre parametri che giustificano l'ingerenza nella vita privata dei cittadini ovvero: l'esistenza di una base giuridica appropriata; la finalità legittima e la necessità in una società

[24] La neutralità tecnica appare peraltro in linea con la giurisprudenza della Corte Costituzionale, secondo cui le risultanze delle operazioni intercettive con captatore non potrebbero tacciarsi di incostituzionalità: si ricordi la sentenza della Corte Costituzionale n. 135 del 2002 nella quale si affermò come il riferimento dell'art. 14 Cost. alle *ispezioni, perquisizioni e sequestri* non fosse espressione di una volontà di tipizzare le limitazioni permesse, ma piuttosto di non poter prevedere tutte le forme di limitazione dell'inviolabilità del domicilio, *"non potendo il Costituente tener conto di forme di intrusione divenute attuali solo per effetto dei progressi tecnologici*";

[25] Ad esempio regole per garantire l'immodificabilità del dato acquisito, ad esempio prevedendo una sorta di verbale firmato digitalmente ad ogni modifica operata sui dati; regole per assicurare la conformità dei dati acquisiti con quelli originali, non essendo il dispositivo fisicamente disponibile ed essendo in continuo funzionamento. Anche in questo caso il legislatore dovrebbe prevedere un certificato di originalità accompagnato da un report certificato e non modificabile ad ogni pacchetto dati registrato; regole per garantire la corretta conservazione dei dati acquisiti tramite archiviazione su supporti non riscrivibili;

[26] Si ritiene che la base legale esistente in materia di intercettazioni di cui all'art. 266 ss. c.p.p. e della disciplina derogatoria di cui all'art. 13 d.l. non possa essere considerata sufficiente per soddisfare la riserva di legge prevista dagli artt. 14 e 15 Cost. in virtù delle particolarità tecniche e della rilevante capacità intrusiva dei trojan virus , sicché ciò si tradurrebbe in una mancata attuazione di tali principi con riferimento all'uso dei trojan virus. contrariamente a quanto sostenuto da R. Orlandi, *Osservazioni sul documento redatto dai docenti torinesi di Procedura penale sul problema dei captatori informatici*, in *Arch. Pen.* 25.07.2016; G. Illuminati, *La disciplina*, op. cit. p. 41 osserva come appartiene alla normale evoluzione del diritto di far ricorso, davanti ad una situazione nuova, alle categorie tradizionali, tentando inizialmente di inquadrarla negli schemi già collaudati, anche se in seguito " *l'esigenza di una disciplina più specifica e meno schematica conduce ad una progressiva differenziazione, che costringe a forzare il quadro prestabilito, fino ad uscirne*".

[27] Sui problemi posti dalla iniziale qualificazione del fatto *sub* art. 51, comma 3 bis c.p.p e dalla successiva riqualificazione: S. Quattrocolo, *Riqualificazione del fatto nella sentenza penale e tutela del contradditorio,* Jovene, Napoli, 2011; 135.

democratica[28]. Di particolare importanza per la Corte è proprio il requisito della base giuridica che, nell'orientamento dei giudici europei, rappresenta l'unico strumento capace di dettare regole chiare e precise che permettano ai cittadini di comprendere l'ampiezza ed i limiti del potere di intrusione nella loro sfera privata[29]. Inoltre, la Corte europea richiede che l'uso del mezzo intrusivo, in una società democratica, sia basato su canoni di proporzionalità e sia sottoposta ad un controllo adeguato ed effettivo, con un'espressione volutamente generica che rinvia all'esigenza che sia il giudice *de quo* a fornire una valutazione in concreto del rapporto tra violazione della sfera privata e fine perseguito, proporzionalità che manca quando la prima, seppur minima produce conseguenze sproporzionate sulla vita di una persona[30].

5. I tentativi legislativi di disciplinare il captatore informatico.

La disciplina delle nuove tecnologie captative nel quadro del processo penale appare, al momento, lontano dai requisiti richiesti dalla Convenzione: il riferimento normativo al concetto di captatore da remoto era infatti contenuto nel d.l. n. 7/2015 c.d. *pacchetto terrorismo*[31], che prevedeva l'inserimento, nell'art. 266 bis c.p.p., che l'intercettazione del flusso di comunicazioni relativa a sistemi informatici o telematici avvenisse anche "*tramite strumenti o programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico*", proposta poi stralciata; successivamente, lo stesso testo, fu riproposto alla Camera il 2 dicembre 2015, all'indomani degli attentati a Charlie Hebdo, del gennaio 2015, e al Bataclan del novembre 2015 a conferma di come tale mezzo investigativo sia spesso avvertito dalle istituzioni come la risposta idonea alla minaccia terroristica.

Attualmente, il tema dei captatori informatici è oggetto del disegno di legge n. 2067 in materia di riforma del processo penale proposto dal Governo il 12 dicembre 2014, approvato dalla Camera dei deputati ed attualmente all'esame del Senato[32]. In particolare l'emendamento c.d. *Casson-Cucca* prevede di affidare al Governo l'emanazione di decreti legislativi contenenti disposizioni sui captatori informatici[33]. L'art. 35 del disegno di legge prevede inoltre una serie di principi direttivi che debbono orientare l'esecutivo in materia di captatori, lasciando trasparire talune lacune nonché facendo proprie alcune riflessioni dei giudici della Corte di Cassazione nella sentenza *Scurato* del 2016.

Si prevede infatti che l'attivazione del microfono debba avvenire solo in conseguenza di apposito comando inviato da remoto e non con il solo inserimento del captatore informatico, nel rispetto dei limiti stabiliti nel decreto del giudice: la previsione intende rassicurare gli animi sul fatto che sebbene la tecnologia sia invasiva, è tuttavia controllabile, potendo essere delimitato l'ambito di operatività del virus alle sole operazioni necessarie; tale previsione seguirebbe un regime differenziato per i procedimenti per mafia e terrorismo per i quali l'at-

[28] Corte Edu, *Zakharov c. Russia*, 4 dicembre 2015 §227; Corte Edu, 10 febbraio 2009, *Iordachi and others c. Moldavia*, req. n.25198/02; Corte Edu, 29 maggio 2001, *Taylor – Sabori c. Regno Unito*, req. n. 47114/99.

[29] Corte Edu, *Zakharov c. Russia*, §231 identifica i contenuti che la base legale deve contenere: predeterminazione della tipologia oggetto delle comunicazioni oggetto di intercettazione, ricognizione dei reati per cui tali mezzi invasivi sono applicabili, attribuzione ad un organo indipendente della competenza ad autorizzare le intercettazioni, definizione delle categorie di persone interessate, limiti di durata e procedura da osservare, utilizzazione e conservazione dei dati ottenuti, l'individuazione dei casi in cui occorre distruggerli.

[30] La Corte Edu ha recentemente fatto applicazione, con due esiti diversi, del criterio di proporzionalità richiesto dall'art. 8 Cedu, nei casi Cevat Ozel c. Turquie, 7/06/2016 e Versini-Campinchi and Crasnianinski c. France, 16/06/2016 ; cfr. sul punto A.Gaito, S. Furfaro, op cit, in *Arch. Pen*., 2/2012, 9; F. Caprioli, *Brevi note sul progetto Gratteri di riforma della disciplina delle intercettazioni,* in *Cass. Pen*. 11/2016, 3981 nel quale l'autore ricorda criticamente i contenuti del progetto Gratteri in materia di intercettazioni (presentato dalla *Commissione per l'elaborazione di proposte normative in tema di lotta, anche patrimoniale, alla criminalità organizzata* nominata il 30 maggio 2014 e i cui lavori si sono conclusi il 31 dicembre 2014) e richiama i suddetti criteri di cui all'art. 8 Cedu. L'A. ricorda inoltre come la proposta della Commissione avrebbe esteso anche ai procedimenti per i reati di cui all'art. 266 c.p.p. il regime autorizzativo più blando previsto dalla disciplina derogatoria di cui all'art. 13 d.l. 13 maggio 1981 n. 152 relativo ai reati di criminalità organizzata.

[31] Per una disamina dei principali aspetti della normativa: Aa.Vv., *Il nuovo pacchetto antiterrorismo*, a cura di R.E. Kostoris, F. Viganò, Giappichelli, 2015.

[32] Il disegno di legge n. 2067 continua ad essere fermo in Senato dopo numerosi rinvii alla sua votazione, da ultimo a seguito della caduta del Governo, la sua approvazione è ulteriormente slittata a data da destinarsi: cfr. v.nuti, Dalla legge elettorale ai voucher, l'agenda di Governo e Parlamento all'inizio del 2017, in *il Sole24ore*, 3 gennaio 2017.

[33] Si tratta dell'emendamento c.d. Casson-Cucca proposto in data 3 agosto 2016 al Disegno di legge n. 2067 recante modifiche al codice penale e al codice di procedura penale per il rafforzamento delle garanzie difensive e la durata ragionevole dei processi,: *"È evidente, quindi, che da una parte risulta urgente poter disporre di questa strumentazione a distanza, che tra l'altro viene usata di fatto da anni e anni anche dalle Forze dell'ordine e dalla magistratura, ma dall'altra questo deve assolutamente avvenire nel rispetto delle garanzie costituzionali, con una regolamentazione che ne definisca puntualmente i criteri di ammissibilità e i modi. Una delega viene data, quindi, in questa materia al Governo, proprio per regolamentare la situazione. Si tratta della disciplina dell'effettuazione di operazioni intercettative cosiddette mediante captatore informatico*".

tivazione del dispositivo sarebbe sempre ammessa, dai procedimenti aventi ad oggetto i reati ordinari per i quali l'attivazione del virus nei luoghi di privata dimora sarebbe limitata alla sussistenza di un'attività criminosa in corso: la disposizione riproporrebbe dunque la dicotomia già delineata dalla sentenza Sez. Un. n. 26889/2016[34], non risolvendo però i problemi collegati alla qualificazione del fatto come reato di criminalità organizzata, come già evidenziato con riferimento alla pronuncia stessa, da cui discendono i principali ostacoli nell'identificazione delle operazioni legittime avvenute in luoghi di privata dimora.

Gli emendamenti proposti in Senato prevedono inoltre una serie di garanzie procedurali, quali la previsione che la registrazione audio venga avviata da determinati soggetti, quali la polizia giudiziaria o il personale incaricato da questa, previa indicazione dell'ora di inizio e di fine della registrazione, e che l'operazione sia verbalizzata; che il trasferimento delle registrazioni sia effettuato soltanto verso il server della Procura, così da garantire originalità ed integrità delle registrazioni, e che al termine della registrazione il captatore informatico debba essere disattivato e reso definitivamente inutilizzabile su indicazione del personale di polizia giudiziaria operante; che vengano utilizzati soltanto programmi informatici conformi a requisiti tecnici (stabiliti con decreto ministeriale da emanarsi entro 30 giorni dalla data di entrata in vigore dei decreti legislativi di attuazione), che garantiscano che tale programma effettui le operazioni espressamente disposte secondo standard idonei di affidabilità tecnica, sicurezza ed efficacia; si prevede inoltre che i risultati delle operazioni, oltre a poter essere utilizzati a fini di prova dei reati oggetto del provvedimento autorizzativo, possano esserlo anche in procedimenti diversi, a condizione che siano indispensabili per l'accertamento dei delitti per i quali è previsto l'arresto obbligatorio in flagranza (*ex* art. 380 c.p.p.): trattasi di una disposizione che allarga pericolosamente l'utilizzabilità dei risultati ad altri procedimenti, senza alcuna garanzia particolare per l'indagato; infine è previsto che non siano in alcun modo conoscibili, divulgabili e pubblicabili i risultati di intercettazioni che abbiano coinvolto occasionalmente soggetti estranei ai fatti per cui si procede, ma la norma non specifica in alcun modo come tale previsione possa essere effettivamente attuata, ad esempio imponendo una previa verifica dei risultati ottenuti da una commissione indipendente, destinata a stralciare i risultati non attinenti.

Durante la discussione in Senato sono state sottolineate alcune lacune che dovrebbero essere integrate per offrire un impianto legislativo maggiormente garantista, tra cui l'esigenza di prevedere misure che eliminino completamente la possibilità di delegare la materiale esecuzione delle operazioni a società private produttrici di *software* spia, dovendo la legge chiarire in maniera incontrovertibile che tale attività è svolta esclusivamente sotto la diretta responsabilità dell'autorità giudiziaria e con la vigilanza della polizia giudiziaria, nel rispetto del decreto del giudice; la mancata previsione puntuale di una catena di operazioni rigorosamente da svolgere per assicurare la legittimità delle captazioni, come è stato fatto, ad esempio, in materia di prelievo coattivo di campioni biologici; nessun riferimento è fatto alla creazione di un albo di esperti nell'utilizzo dei virus *trojan*, nonché di un registro nazionale dei captatori che garantisca standard idonei circa la loro omologazione e sistemi di verifica della loro conformità al dettato normativo al fine di garantire la corretta manipolazione e conservazione dei dati acquisiti; nulla è detto inoltre sull'attribuzione alla parte processuale del diritto di ottenere la documentazione relativa a tutte le operazioni svolte con captatore e il diritto di chiedere al giudice la verifica dei requisiti di conformità legale del captatore informatico che, come detto in precedenza, dovranno essere anch'essi essere indicati.

6. Uno sguardo alla disciplina dei captatori informatici nell'esperienza europea.

Giova inoltre offrire uno sguardo a come il tema dei captatori sia disciplinato in alcuni altri Paesi europei, in particolare in Germania e in Francia.

[34] Viene infatti previsto, sempre con riferimento alla criminalità organizzata, la possibilità per il Pm di disporre le intercettazioni mediante agente intrusore in casi concreti di urgenza poi successivamente sottoposti a convalida del giudice entro quarantotto ora e sempre che il decreto sia motivato sia in ordine alle specifiche ragioni di urgenza sia in ordine alla necessità di disporre quella specifica modalità di intercettazione.

E' del 20 aprile 2016 l'importante sentenza con cui il Tribunale Costituzionale tedesco[35] dichiarava la parziale illegittimità costituzionale di alcune disposizioni contenute nella legge che regolamenta i compiti della polizia federale con riferimento all'uso di tecnologie particolarmente invasive della *privacy* dei cittadini.

Due punti sembrano fondamentali nella pronuncia della Suprema corte tedesca. Il primo: la Corte sanciva che è condizione necessaria per disporre mezzi di sorveglianza in luoghi diversi dal domicilio al fine di prevenire la commissione di reati la prevedibilità del compimento di uno specifico reato, tramite l'identificazione perlomeno della sua natura e la previsione che il comportamento della persona si traduca nel compimento di fatti riconducibili a quel reato nel prossimo futuro. In secondo luogo, con riferimento alle operazioni di sorveglianza in case private, la Corte suprema tedesca chiariva che il principio di proporzionalità è solo parzialmente soddisfatto quando le operazioni coinvolgono accidentalmente anche terze persone, perché in tal caso il loro diritto alla riservatezza viene violato. Per tale ragione, la Corte esigeva che i dati raccolti siano analizzati da un organismo indipendente prima di essere affidati alla polizia federale, al fine di eliminare qualsiasi informazione non attinente alle operazioni.

Questa sentenza seguiva un'altra importante decisione del 27 febbraio 2008[36] con cui la Corte suprema tedesca aveva già coniato un vero e proprio diritto costituzionale alle garanzie di integrità e di riservatezza dei sistemi informatici, enucleazione del diritto alla dignità dell'individuo nello spazio digitale.

Anche in Francia la materia delle intercettazioni è articolata su un doppio binario: da un lato, l'art. 100 ss. del Code de procédure pénal relativo ai procedimenti ordinari che prevede che sia il *juge d'instruction* a disporre operazioni intercettive in procedimenti per *délits o crimes* puniti con più di due anni di reclusione e per una durata di quattro mesi rinnovabile, dall'altro, a seguito della legge 9 marzo 2004 è possibile disporre intercettazioni preventive sulla base di una disciplina derogatoria prevista dall'art. 706-95 c.p.p. in materia di criminalità organizzata – disciplinata nel libro IV del Code de procédure pénale relativo alle procedure particolari[37] – che consente già durante *l'enquête préliminaire* o de *flagrance* di ricorrere alle operazioni di intercettazione. In tal caso le operazioni sono autorizzate dal *juge des libertés et de la détention* su domanda al *Procureur de la République* e le operazioni possono avere una durata di un mese rinnovabile una volta.

Ora, con riferimento alla disciplina derogatoria in materia di criminalità organizzata, il legislatore è intervenuto prevedendo all'art. 706-96 c.p.p. le c.d. "*sonorisations et fixations d'images de certains lieux ou véhicules*" e all'art. 706-102-1 c.p.p. la c.d."*captation des données informatiques*", entrambe applicabili con riferimento all'elenco di reati previsti dagli artt. 706-73 e 706-73-1 c.p.p., che a loro volta richiamano i *crimes et delits* costituenti atti di terrorismo ai sensi degli artt. 421-1 à 421-6 del Code pénal.

L'art. 706-96 c.p.p. consente, in particolare, la captazione delle parole pronunciate da due o più persone in maniera confidenziale, in un luogo o veicolo pubblico o privato mediante l'inserimento di un dispositivo tecnico all'insaputa dell'utente, autorizzato dal *juge d'instruction*, su parere favorevole del *Procureur de la République* ; in particolare gli articoli del *Code de procédure pénal* prevedono alcune garanzie procedurali che debbono essere adempiute dagli operatori quali ad esempio la redazione di un verbale di tutte le operazioni (art. 706-100 c.p.p.) o la distruzione dei dati acquisiti, quando l'azione penale non può più essere esercitata (art. 706-102 c.p.p.); l'art. 706-96 c.p.p. ha riproposto, anche oltralpe, il problema della riconducibilità dei fatti oggetto del procedimento a quelli di cui all'art. 706-73 ss. c.p.p. in materia di criminalità organizzata, e comunque, a seguito di una nota condanna della Francia da parte della Corte

[35] Bundersverfassungsgericht, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09; A. Venegoni-L. Giordano, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo strumenti informatici*, in *Dir. pen. cont.*, 8 maggio 2016.

[36] **S**entenza del Bundesverfassungsgericht del 27 febbraio 2008 sulla c.d. online durchsuchung, in *Riv. trim. dir. pen. econ.*, 3, 2009, pag. 679 e ss., con nota di R. Flor, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung*.

[37] Da ultimo alcune modifiche alla disciplina derogatoria sono state apportate dalla Loi del 3 juin 2016 sulla lotta contro il terrorismo, sulle novità introdotte da quest'ultimo testo: cfr. O. Decima, *Terreur et methamorphose,* D. 2016,1826 ; M. Quemener, *Les techniques spéciales d'enquête en matière de lutte contre la cybercriminalité,* in *AJ Penal,* 2015, 403, id, *Les dispositions liées au numériques de la loi 3 juin 2016 renforçant la lutte contre le crime organisé et le terrorisme,* in *Dalloz* IP/IT, 2016,431 ; S. Hennequin, *Quid la captation de donnés informatiques*?, D. 2001.1358.

europea[38], la norma prevede, anche nell'ambito della disciplina derogatoria, il divieto di procedere alla captazione in determinati luoghi privati quali studi legali, ordine forensi, luoghi deputati ad esercitare attività giornalistica, domicilio dei giornalisti, studi di notai, ufficiali giudiziari, magistrati, senatori, deputati.

L'art. 706-102-1 c.p.p. disciplina invece la c.d."*captation des données informatiques*" che consente, sempre tramite dispositivo inoculato su un supporto informatico, l'accesso a tutte le informazioni dell'utente ivi presenti e il compimento di una serie di attività di salvataggio, stoccaggio e trasmissione di tali dati[39]. Anche in tal caso gli articoli seguenti del Code de procédure pénal prevedono una serie di indicazioni sulle modalità con cui tali operazioni devono essere effettuate, quali ad esempio l'obbligo per il giudice, a pena di nullità, di precisare il reato che giustifica il ricorso a tale mezzo informatico, la localizzazione esatta o la descrizione del sistema informatico e la durata delle operazioni (art. 706-102-3 c.p.p.). Il secondo comma dell'articolo 706-102-1 c.p.p. è stato inoltre modificato prevedendo la creazione di liste di tecnici esperti presso la *Cour de Cassation* e le *Cours d'appel* a cui affidare il compito di compiere le operazioni con captatore informatico. È stato inoltre emanato il *Décret n° 2015-1700* del 18 dicembre 2015 che, dando attuazione all'articolo 706-102-1 c.p.p. ha disciplinato alcune garanzie procedurali nell'uso dei dispositivi informatici, senza che però lo si possa considerare esaustivo in materia: il decreto identifica i soggetti che hanno accesso ai dati raccolti, le operazioni da compiere per la validità degli stessi, il termine entro il quale i dati devono essere distrutti, le modalità di loro conservazione, l'autorità a cui rivolgersi per l'accesso e la rettifica delle informazioni raccolte.

Si ricorda infine che la legge n.731 del 3 giugno 2016 introduceva, agli artt. 706-95-4 e seguenti del Code de procédure pénale, una specifica disciplina dell'IMSI *catcher*, altro strumento tecnologico, simile ad un antenna, che permette di captare e localizzare il numero di telefono e che, nelle versioni più aggiornate, può anche permettere di intercettare dati[40].

7. Considerazioni conclusive.

Questi brevi cenni a quanto accade nei Paesi a noi vicini confermano come la necessità di ricorrere a strumenti tecnici innovativi per combattere il crimine organizzato e il terrorismo sia un'esigenza avvertita uniformemente all'interno dei vari ordinamenti europei. Tuttavia è bene ricordare che l'esigenza di lottare contro tali fenomeni può essere considerata legittima solo quando proporzionata allo scopo che si persegue in una società *democratica*, laddove tale ultimo aggettivo costituisce la premessa, e al tempo stesso, il termine ultimo di comparazione a cui l'agire dello Stato deve conformarsi quando ricorre a strumenti di grande invasività, quali quelli qui esaminati.

D'altronde, che i captatori informatici - e con essi tutti gli altri strumenti informatici che man mano si affermeranno con il progresso tecnologico – siano utili e non debbano essere demonizzati appare incontestabile: è proprio la loro natura itinerante a renderli armi essenziali nella lotta che le nostre società debbono condurre contro il terrorismo.

La sensazione è che, tuttavia, contro crimini di tal genere la capacità reattiva dell'ordinamento sia la sola che possa, molto spesso, rivelarsi decisiva per salvare l'incolumità degli individui; essendo dunque impensabile, né auspicabile, che i Paesi smettano di far ricorso a strumenti di tale reattività ed utilità, la soluzione – in uno Stato di diritto – non può che passare dal bandire un uso "sotterraneo" di tali mezzi e dall'offrire, o perlomeno dal tentare di offrire, un quadro legislativo capace di arginare i rischi di abusi investigativi e processuali. Come i riferimenti alla Germania e alla Francia dimostrano, la consapevolezza della necessità di tali strumenti non consente di rinnegare la necessità di un bilanciamento essenziale con

[38] Sull'art. 706-96 c.p.p. e la sua applicazione a luoghi privati: Corte Edu, Wisse c. Francia, 20 marzo 2006 ; Corte Edu Vettel c. France, 31 maggio 2005, in materia di *sonorisation* di un appartamento prima dell'entrata in vigore della legge del 9 marzo 2004 in materia di criminalità organizzata; cfr. H. VLAMYNCK, *Le point sur la captation de l'image et des paroles dans l'enquête de police*, in *AJ Pénal*, 2011-574; T. POTASZKIN, *Précisions sur les mesures de sonorisation et de fixations d'images*, *D.* 2013.1045.

[39] B. BOULOC, *Procédure pénale*, Dalloz, 25 ed. p. 694 ss : cfr. A.BAUER – C. SOULLEZ, voix *Terrorismes*, Dalloz, 2015, 96 F. CHOPIN, *Cybercriminalité*, in *Rep. droit pén. proc. pén.*, D. 2016.

[40] L'IMSI Catcher è un dispositivo elettronico che si comporta come una falsa antenna e che entra in comunicazione con telefoni, tablets, personal computers per captare informazioni nel suo raggio di azione : in particolare vengono recepiti elementi tecnologici della connessione come numeri di telefono, identità di chi li emette, destinatari delle chiamate, localizzazione. Alcuni dispositivi possono anche captare il contenuto delle comunicazioni : cfr. E. VERGES, *La procédure pénale à son point d'équilibre*, in *RSC* 2016, 551.

altri valori fondamentali delle nostre società, aprendo dunque un dibattito di ampio respiro a livello nazionale ed europeo, destinato a modificare la nozione di riservatezza nelle società in cui viviamo.

Il polverone sollevato dalla questione dell'uso dei captatori informatici e di strumenti tecnici sempre più sofisticati, non può essere relegato a mero *fenomeno passeggero*, a cui obbiettare che domani seguiranno altri e più evoluti ancora sistemi informatici di maniera che il sistema legislativo non sarà mai in grado di offrire una tutela completa ed esaustiva: d'altronde il diritto è scienza in costante evoluzione, forgiato da secoli di riflessioni, mai sazio degli obbiettivi raggiunti, ma sempre alla ricerca di un punto di equilibrio che traduca un bilanciamento tra esigenze meritevoli di tutela[41].

Lo Stato dunque che non può e non deve rinunciare al primordiale istinto di autoconservazione contro attacchi alla sicurezza comune, deve agire nella consapevolezza che la comprensione dei diritti fondamentali, rappresentando essi un limite invalicabile al potere dell'autorità pubblica, può essere ammessa solo se posta in essere in un quadro imperativamente determinato dal legislatore. Egli è pertanto chiamato a formulare una disciplina quanto più organica e completa possibile all'uso di nuovi strumenti tecnici, quali tra essi i captatori, non solo con riferimento alle operazioni di intercettazione, ma più generalmente in relazione a tutte le ulteriori operazioni che con tali strumenti sia possibile eseguire, al fine di garantirne l'impiego in un quadro legislativamente definito, eliminando, nella maggior misura possibile, zone d'ombra per la tutela dei singoli.

[41] G. Lumia, *Scienze umane e sapere giuridico*, in *La giustizia penale e la fluidità del sapere*, Cedam, 1988, 12: che vede nel diritto uno strumento di integrazione sociale e nel giurista colui che deve costruire una macchina sociale capace di prevedere o almeno soffocare i conflitti tra interessi contrapposti che animano la società.