AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

I programmi spia: il diritto alla privacy di fronte ai nuovi strumenti tecnologici di indagine

di Michela Tresca*

Sommario: 1. L'ammissibilità dei programmi spia quali mezzi di ricerca della prova. 2. La sentenza 28 aprile 2016 delle Sezioni Unite della Corte di Cassazione: il nuovo approccio in materia di "captatore informatico". 3. La sentenza 20 aprile 2016 del Bundesverfasungsgericht: l'approccio tedesco in materia. 4. Conclusioni

1. L'ammissibilità dei programmi spia quali mezzi di ricerca della prova

Il tema dell'utilizzo di strumenti informatici quali mezzi di ricerca della prova all'interno di indagini risulta connesso a questioni assai ampie che abbracciano, almeno, due distinti ambiti[1]. Da un lato, lo sviluppo delle tecnologie dell'informazione e della comunicazione ha messo a disposizione strumenti sempre più invasivi del diritto alla riservatezza dell'individuo, non solo con riferimento alla facilità di accesso alle tipologie di dati che possono essere captati, memorizzati e copiati, ma anche all'estensione di tale intrusione, con il rischio di giungere a veri e propri sistemi di sorveglianza di massa. Dall'altro, vi è la questione connessa alla mole di dati che circolano in rete e all'uso dei suddetti strumenti per la commissione di frodi informatiche, ma anche di altri reati perpetrati offline.

Tra le potenzialità offerte dalle nuove tecnologie, assumono un rilievo giuridico particolare i così detti "trojan horse" o anche "captatori informatici"[2], vale a dire *malware* che, installati su un dispositivo all'insaputa dell'utente/proprietario, permettono di gestire da remoto il sistema informatico, sia in termini di contenuti in esso memorizzati e immessi, sia in termini di controllo delle funzionalità del mezzo.

* Collaboratrice stabile di @LawLab - Laboratorio sul Diritto del Digitale, Luiss Guido Carli.

[1] In questo senso, cfr. E. M. CATALANO, *Prassi devianti e prassi virtuose in materia di intercettazioni, Editoriale,* in *Processo penale e giustizia* n.1, 2016.

[2] Per un'illustrazione di tali strumenti, v. S. COLAIOCCO*, Nuovi mezzi di ricerca della prova: l'utilizzo dei programmi spia,* in *Archivio penale* n. 1, 2014.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Si tratta, quindi, di un programma spia che si presenta sotto due tipologie principali: l'"*online search"* o "*one time copy*", che consiste nella captazione del contenuto del sistema informativo, e si risolve nella possibilità di copiare o memorizzare dati presenti nel dispositivo; e l'"*online surveillance*" che invece riguarda la captazione del flusso telematico dei dati tra il sistema in questione e altre periferiche, e si risolve nella possibilità di accedere a tutte le funzionalità, tra cui l'attivazione del microfono o della telecamera, e l'accesso a ciò che viene visualizzato sullo schermo. Tali programmi spia possono essere inseriti sia da remoto attraverso *virus trojan,* sia agendo fisicamente sull'*hardware* del mezzo da sottoporre a intercettazione.

Al di là delle specifiche tecniche di tali strumenti, rileva in questa sede verificare la loro ammissibilità all'interno del nostro ordinamento giuridico. Ad oggi, nel silenzio del legislatore, tale verifica è stato svolta dalla giurisprudenza che - per evitare di definire illegittimo il ricorso a strumenti così innovativi - ha tentato di ricondurli, talora, all'ambito delle prove atipiche di cui all'art. 189 c.p.p[3], talaltra, invece, nel campo delle intercettazioni, e quindi sempre all'interno del quadro codicistico dedicato ai mezzi di ricerca della prova (artt. 266 ss., c.p.p.).

Entrambe queste ricostruzioni non hanno mancato, tuttavia, di destare dubbi e perplessità, che derivano innanzitutto dall'ontologica differenza tra mezzi tradizionali, a cui si riferisce la normativa menzionata, e le peculiarità dei nuovi strumenti che si avvalgono del supporto informatico[4]. A tali considerazioni critiche, se ne sono aggiunte altre in occasione dell'approvazione del d.l. antiterrorismo[5], che ha introdotto una serie di modifiche al codice penale, al codice di procedura penale e al Codice della privacy. Non può essere sottovalutato il clima entro cui si è svolto il dibattito, caratterizzato da un contesto dominato dalla minaccia

[3] L'art. 189 c.p.p. così statuisce «Quando è richiesta una prova non disciplinata dalla legge, il giudice può assumerla se essa risulta idonea ad assicurare l'accertamento dei fatti e non pregiudica la libertà morale della persona. Il giudice provvede all'ammissione, sentite le parti sulle modalità di assunzione della prova.».

[4] Su questo occorre tener presente come il software spia si basa su una delega del P.M. a tecnici nominati ausiliari di polizia giudiziaria, la cui attività potrebbe uscire dal controllo tanto del P.M. quanto della p.g. Il ruolo del P.M si risolve nel concedere il decreto di autorizzazione, che comunque è carente in merito alla utilizzabilità delle intercettazioni in base alle modalità esecutive richieste dall'art. 271, comma 1 , c.p.p. A ciò si aggiunge che non è sempre possibile ritenere che la p.g. sovraintenda alle attività di captazione poste in essere dal tecnico ed è totalmente rimessa nelle mani di quest'ultimo l'attività di captazione da remoto, non essendo necessario - come nel caso delle intercettazioni tradizionali - una collaborazione di un terzo (gestore telefonico).

[5] D. l. n. 7 del 18 febbraio 2015, convertito in l. n. 43 del 17 aprile 2015 (in G.U. n. 91 del 20 aprile 2015).

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

terroristica, divenuta più che mai attuale in seguito agli attentati di Charlie Hebdo del 7 gennaio 2015. Pur non rinvenendosi riferimento alcuno nel testo iniziale a strumenti quali il "captatore informatico", è nel progetto proposto dalle Commissioni che era stata successivamente introdotta la possibilità di accesso da remoto nei dispositivi informatici, attraverso il ricorso a software spia, con una modifica rilevante all'art. 266 bis c.p.p.[6]. Nel testo finale del decreto è stata, infine, stralciata tale norma, alla luce dell'avvertita necessità di dedicare una maggiore riflessione al tema[7].

La previsione tanto dibattuta, e stralciata dalla versione finale del decreto su menzionato, sembra ora aver trovato una nuova collocazione all'interno della proposta di legge A.C. n. 3470 del 2 dicembre 2015 *di modifica all'articolo 266-bis del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche*, e quindi reinserita all'interno del più generale dibattito in materia di intercettazioni.

Il quadro appena esposto rende chiara la complessità della questione, soprattutto di fronte a strumenti e modalità di indagine che alla luce delle grandi potenzialità - sia in termini di intrusività che di efficacia nella ricerca della prova - non trovano disciplina a livello normativo, circostanza che contribuisce a rendere particolarmente indefiniti i confini circa la legittimità di una loro effettiva utilizzazione.

[6] L'art. 2 comma 1-ter del testo proposto dalle commissioni prevedeva, infatti, quanto segue: «al codice di procedura penale sono apportate le seguenti modificazioni: a) all'art. *266-bis,* comma 1 ("'1. Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi" sono aggiunte le seguenti parole: ",anche attraverso l'impiego di strumenti e di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico"».

[7] Sul punto non erano tardate a farsi sentire le preoccupazioni espresse dal Garante privacy, il quale rilevava, nel testo del decreto, un'assenza di proporzionalità tra le due opposte esigenze di assicurare la sicurezza dei cittadini e al tempo stesso garantire il loro diritto alla protezione dei dati e che di fatto sembrava contrastare la posizione espressa dalla CGUE con la Sentenza *Digital Rights Ireland* dell'aprile del 2014; cfr. Soro: seria preoccupazione per emendamenti approvati a DL antiterrorismo – 24 marzo 2015, su *www.garanteprivacy.it.*

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

2. La sentenza 28 aprile 2016 delle Sezioni Unite della Corte di Cassazione: il nuovo approccio in materia di "captatore informatico"

La sentenza del 28 aprile 2016 chiarisce la posizione assunta, da ultimo, dalle Sezioni Unite della Suprema Corte in materia di indagini effettuate mediante "captatore informatico", proprio al fine di dirimere i dubbi sull'ammissibilità di tali strumenti.

La questione posta davanti alla Corte riguarda essenzialmente la legittimità del ricorso al trojan horse in luoghi di privata dimora ai sensi dell'art. 614 c.p. e la sussistenza, in tali casi, della necessità di una indicazione preventiva, all'interno del decreto di autorizzazione, circa i luoghi nei quali l'intercettazione viene effettuata.

La controversia si colloca all'interno di un'indagine sulla criminalità organizzata, avviato presso la Procura di Palermo, nell'ambito della quale era stata disposta l'installazione di un captatore informatico su un dispositivo che avrebbe permesso di effettuare intercettazioni anche nell'ambito dell'abitazione dell'intercettato[8]. Proprio contro il provvedimento di autorizzazione, la difesa lamentava che si sarebbe in questo modo permessa un'intercettazione anche in luoghi privati – senza, peraltro, specificare se in quei luoghi avvenisse l'attività illecita - e che il provvedimento risultava troppo generico, giacché consentiva di effettuare intercettazioni in qualsiasi luogo si fosse recato il soggetto. Su tali punti, il Tribunale del riesame di Palermo rilevava che, trattandosi di un procedimento "per fatti di mafia", non si sarebbe resa necessaria la verifica circa il compimento di attività criminale nella dimora privata; inoltre, il decreto di autorizzazione del g.i.p. forniva limiti idonei ad evitare una intrusione indiscriminata nella sfera di riservatezza dell'intercettato[9]. Contro l'ordinanza del Tribunale di Palermo, la difesa aveva promosso ricorso in Cassazione.

Non condividendo le conclusioni espresse dalla stessa Suprema Corte, sez. VI, nella sentenza 2700/2015, e volendo evitare conflitti di interpretazione, il Collegio rimetteva la questione

[8] Per un primo commento alla sentenza v. M. T. ABBAGNALE, *In tema di captatore informatico,* in *Archivio penale* 2016, n. 2.

[9] Per un commento alla sentenza del Tribunale di Palermo, si rimanda a G. NEGRI, *Intercettazioni, via libera alle microspie nei tablet,* in *www.ilsole24ore.com,* 7 aprile 2016 e a E. LORENZETTO, *Il perimetro delle intercettazioni ambientali eseguite mediante "captatore informatico",* in *www.penalecontemporaneo.it,* 24 marzo 2016, la quale sottolinea l'equivoco in cui cade il giudice nel definire specifico un luogo che in realtà non lo era e non convince il riferimento al luogo domestico dato che la peculiarità dello strumento in cui è inserito il trojan – un telefono cellulare- permette, proprio perché mobile, di essere utilizzato anche in luoghi diversi dal domicilio dell'indagato.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

davanti alle Sezioni Unite. Tre sono essenzialmente le questioni individuate nell'ambito dell'ordinanza di remissione[10]: innanzitutto se il decreto di autorizzazione deve fornire indicazione dei luoghi in cui si prevede di effettuare l'intercettazione; in secondo luogo, se, nel caso non risultasse l'indicazione, sarebbero colpite dalla sanzione di inutilizzabilità solo le captazioni effettuate nei luoghi di privata dimora; infine, se, nel caso di indagini sulla criminalità organizzata, si può in ogni caso prescindere dalla indicazione dei luoghi. La posizione espressa nell'ordinanza di remissione conduce a ritenere le intercettazioni effettuate con "captatore informatico" all'interno di procedimenti attinenti alla criminalità organizzata come intercettazioni "tra presenti", per le quali non sarebbe necessario specificare il luogo in cui avvengono.

Nella sentenza in commento, le Sezioni Unite, contrariamente a quanto disposto dalla Sezione VI nel 2015, hanno riconosciuto la possibilità di dar luogo a intercettazioni tramite l'utilizzo di "captatore informatico" anche in luoghi rientranti nella dimora privata e senza la necessità di indicare preventivamente, nel decreto di autorizzazione, i luoghi di effettuazione, con il solo requisito di doversi trattare di un procedimento contro la criminalità organizzata[11]. Proprio con riferimento alla nozione di "delitti di criminalità organizzata", la Corte, disattendendo quanto auspicato dalla Procura generale, sembra abbracciare una interpretazione particolarmente ampia che ricomprende tra i reati di criminalità organizzata «qualsiasi tipo di associazione per delinquere, ex art. 416 c.p.».

Si può notare come la Suprema Corte, nel riconoscere – entro i limiti indicati – il ricorso ai così detti "Trojan di Stato", non sembra porsi il problema della legittimità in sé dello strumento, che pure potrebbe destare preoccupazioni quanto al suo potenziale di intrusività; essa si sofferma, piuttosto, a delineare un limite per il ricorso a tale strumento nella "inviolabilità del domicilio", nel caso di intercettazioni ambientali effettuate attraverso

[10] Cass., Sez. VI, (ord.) 6 aprile 2016, n. 13884.

[11] In senso critico alle conclusioni della Corte, v. L. FILIPPI, *Il captatore informatico: l'intercettazione ubicumque al vaglio delle Sezioni Unite,* in *Archivio penale* 2016, n.1, *Osservatorio della Corte di Cassazione,* il quale mostra come il ricorso a captatori informatici come autorizzazione di una generica intercettazione ambientale si presenterebbe in violazione del diritto interno (a partire dall'art. 15 della Cost., ma anche degli artt. 266 e 267 c.p.p) della normativa europea e internazionale e della giurisprudenza della Corte EDU di cui si richiama una pronuncia del 2009 (*Iordachi e altri c. Moldavia*) con cui si dispone il criterio della "prevedibilità" delle misure segrete di sorveglianza.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

l'attivazione del microfono del dispositivo in questione[12]. In questo modo, la Corte sembra affrontare la questione solo alla luce della tutela apprestata dall'art. 14 Cost., quando invece il tema pare riguardare la tutela dell'individuo nel suo complesso, anche guardando oggi alla sua presenza in rete e al suo "corpo digitale".

Al di là dell'ultimo caso affrontato dalla Corte, le pronunce della giurisprudenza italiana in merito al ricorso a simili strumenti di indagine, caratterizzati da una intrusività senza precedenti, sono ovviamente piuttosto recenti e poco numerose. Una breve ricostruzione della posizione del giudice di legittimità può dare l'dea di come la giurisprudenza abbia interpretato in questi anni la natura di strumenti quali i software spia e sulla conseguente legittimità del ricorso ad essi. Tra le prime pronunce, può essere segnalata la sentenza *Virruso* del 2009[13] in cui la Corte ricondurrà il captatore informatico alla categoria delle "prove atipiche" ex art. 189 c.p.p.[14], dal momento che l'attività di investigazione posta in essere si era risolta nel prelevare e copiare documenti memorizzati nell'hard disk del dispositivo, e consisteva in «una relazione operativa tra microprocessore e video del sistema elettronico». Attraverso il ricorso a tale strumento non si era quindi proceduto alla captazione di un "flusso di comunicazione", ma si aveva avuto accesso, da remoto, ai dati e ai contenuti memorizzati sul computer. Al riguardo, è da notare che il decreto di autorizzazione non aveva disposto solo la possibilità di copiare i contenuti già presenti nel dispositivo in questione, ma anche quella di acquisire i contenuti che sarebbero stati inseriti in un momento successivo, potendosi effettuare tale captazione anche in tempo reale. L'utilizzo di tale strumento non avrebbeviolato, secondo la Corte, gli art. 14 e 15 della Costituzione[15], anche perché il luogo in

[12] In questo senso C. BLENGINO, *Trojan a domicilio,* in *www.ilpost.it,* 3 maggio 2016.
[13] Cass., Sez. V, 14 ottobre 2009, Virruso, in *Mass. Uff*., n. 246955; si tratta di un caso all'interno di un'indagine in cui si dispone l'autorizzazione per la Polizia di Stato di poter accedere al computer dell'indagato collocato nel luogo di lavoro – un ufficio pubblico comunale – attraverso il ricorso a un software spia; v. su questo S. COLAIOCCO, *cit*.
[14] In merito alla possibilità di far rientrare prove di indagini all'interno dell'art. 189 c.p.p. si era già espressa la Corte di Cassazione nel caso *Prisco;* v. SS. UU., sent. 28 luglio 2006, n. 26795, in cui si affronta la questione delle riprese video nei luoghi di privata dimora. Dalle argomentazioni della Corte si può dedurre come l'art. 189 pur ammettendo, in presenza di determinate circostanze, l'ingresso di alcune prove non previste dalla legge, non può essere letto nel senso che si possa in ogni caso riconoscere l'ammissibilità di qualsiasi attività posta in essere a scopi investigativi, ma solo di quelle lecite e che non costituiscono reato.
[15] Gli artt. 14 e 15 Cost. disciplinano, rispettivamente, l'inviolabilità del domicilio e la segretezza della corrispondenza.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

cui era collocato il computer – un ufficio pubblico comunale - non sarebbe ricaduto nella nozione di "privata dimora". In definitiva, facendo rientrare lo strumento utilizzato tra le prove atipiche, la Corte lo sottrae di fatto alle previsioni di cui all'art. 266 c.p.p.. In un caso successivo[16], il ricorso a software spia per accedere al contenuto presente nel computer dell'indagato non è ricondotto all'ambito delle intercettazioni, rimanendo così sulla scia di quanto rilevato in precedenza.

Come già accennato, argomentazioni diverse da quelle espresse nell'ambito della sentenza in delle Sezioni Unite in commento erano state addotte dalla Corte di Cassazione nel 2015[17], circa la riconducibilità dei captatori informatici all'interno delle intercettazioni ambientali e quindi alla disciplina di cui all'art. 266, co. 2, c.p.p.

La Corte si pronunciò, in particolare, su due questioni. La prima riguardava l'attivazione da remoto del microfono dello smartphone; la seconda concerneva, invece, la questione dell'attivazione, sempre da remoto, della videocamera del cellulare. Sul primo punto, la Suprema Corte concluse per la non ammissibilità di un tale strumento alla luce del quadro normativo dato che, rispetto alle intercettazioni tradizionali, esso avrebbe permesso di effettuare la captazione della comunicazione in qualsiasi luogo e avrebbe imposto, quindi, l'indicazione precisa del luogo in cui sarebbe stata effettuata nell'ambito del decreto di autorizzazione. Per la seconda questione, la Suprema Corte ritenne che, alla luce della

[16] Si tratta del caso *Bisignani,* Cass., Sez. VI, 27 novembre 2012, in *Mass. Uff.,* n. 254865; il caso si colloca all'interno di un'indagine su una presunta associazione di stampo P4, avviata dalla procura della Repubblica presso il Tribunale di Napoli; nel caso di specie il ricorso al software spia non solo aveva permesso di avere accesso ai dati memorizzati nell'hardware del sistema informatico sotto controllo, ma anche di effettuare intercettazioni ambientali attraverso il controllo della videocamera e del microfono del dispositivo. Per quest'ultimo caso, il g.i.p dispone l'autorizzazione ex art. 267 c.p.p. facendo rientrare tale attività all'interno delle intercettazioni ambientali; quanto alla prima attività – vale a dire ricorso al software anche nel senso di *online search*- rimanendo in linea con quanto disposto dalla Cassazione nel 2010, ritiene sufficiente a garantire la riservatezza dei soggetti interessati il provvedimento del P.M..

[17] Cass., Sez. VI, 26 maggio 2015, *Musumeci,* in *Guida dir.,* n. 41, 2015, 83; in Cassazione si contesta l'ordinanza del Tribunale del riesame di Catania di conferma della ordinanza applicativa della misura intramurale per il reato ex art. 416 bis c.p, per partecipazione di tipo mafioso. Il ricorrente lamenta, per quel che in questa sede interessa, con il secondo e terzo motivo – violazione di legge e vizio di motivazione -, l'ammissibilità di misure di intercettazione effettuate tramite software spia e che avrebbero permesso sia l'accesso ai dati contenuti nel telefono cellulare in questione, sia l'attivazione del microfono del dispositivo, avendo quindi anche luogo intercettazioni tra presenti. Si sarebbe così giunti a una captazione illegittima e invasiva dei contenuti in violazione dell'art. 8 CEDU.

giurisprudenza prevalente in materia, occorresse verificare che le videoriprese non fossero state effettuate in un luogo privato. Da tali presupposti, la Corte fece discendere la necessità di un'indicazione preventiva dei luoghi in cui effettuare le intercettazioni, nonché una previsione circoscritta degli stessi, non potendosi fornire una lettura estensiva della disposizione alla luce dell'art. 15 Cost., che, in deroga alla inviolabilità della segretezza della corrispondenza, prevede specifici limiti di motivazione nell'atto dell'autorità giudiziaria e nelle garanzie stabilite dalla legge[18]. La necessità di una tale interpretazione restrittiva trovava, per la Corte, un'ulteriore conferma nella peculiarità del mezzo, che «aggiunge un quid pluris, rispetto alle ordinarie potenzialità delle intercettazioni, 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 limitazioni di luogo.». In definitiva, dunque, nel decreto di autorizzazione avrebbe dovuto rinvenirsi l'indicazione dei luoghi in cui sarebbe stata effettuata l'intercettazione delle comunicazioni tra presenti. La Corte aveva annullato, quindi, l'ordinanza impugnata e aveva rimesso la questione al Tribunale di Catania.

Se con quest'ultima pronuncia la giurisprudenza intendeva fornire un argine al ricorso a software spia nell'ambito di indagini - non riconoscendo in via analogica la riconducibilità di tali strumenti alle previsioni codicistiche - con la sentenza del 28 aprile del 2016, le Sezioni Unite sembrano aver riaperto a un legittimo ricorso a tali strumenti, seppur - nel caso di specie - con specifico riferimento a indagini riguardanti reati per mafia o reati di natura terroristica.

[18] Su tale posizione non è mancata di pronunciarsi in senso critico parte della dottrina; v. in tal senso G. AMATO, *Intercettazioni mediante agenti intrusori, la Cassazione non è al passo con i tempi,* in *www.procuratrento.it,* il quale rileva che, nel giungere alla sua conclusione, la Corte non avesse preso in considerazione le specificità delle intercettazioni ambientali rispetto a quelle telefoniche; per le prime, in cui si fa rientrare il ricorso al captatore informatico, non si fa riferimento all'individuazione uno strumento specifico, quanto ad ambienti, rendendosi sufficiente che nel decreto di autorizzazione siano specificate i contesti ambientali in cui deve svolgersi la captazione.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

3. La sentenza 20 aprile 2016 del Bundesverfassungsgericht: l'approccio tedesco in materia.

La Germania costituisce un esempio interessante in materia essendo stato il primo dei paesi europei ad autorizzare tali forme di intercettazioni di Stato[19], ma anche il primo a mettere in discussione la liceità di simili strumenti, fortemente intrusivi perché in grado di permette l'accesso a una grande quantità di documenti che si trovano sul dispositivo.

È con una sentenza del 2008 del Bundesverfassungsgericht[20] che l'utilizzo dei software spia viene considerato, generalmente, come una violazione dei diritti civili dei cittadini, in quanto configura un controllo "onnipresente" nei confronti di quest'ultimi, da limitare a determinate e specifiche circostanze.

L'importanza della pronuncia è da rinvenire in particolare nel fatto che, per la prima volta nel quadro europeo, si riconosce un nuovo diritto costituzionale che si sostanzierebbe nel "diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici". L'assunto da cui è partito il giudice nel riconoscimento di tale diritto è essenzialmente il ruolo fondamentale ricoperto dalla tecnologia nella società contemporanea e la continua presenza degli individui su tali dispositivi, contesto di fronte al quale il quadro normativo non fornisce, ad opinione della Corte Costituzionale tedesca, adeguata protezione.

Alla luce di tale premesse, la Corte dichiara in contrasto con la Costituzione – e specificatamente con l'art. 10 (segretezza della corrispondenza e delle comunicazioni) e con l'art. 13 (inviolabilità del domicilio) della Grundgesetz - un emendamento apportato nel 2006 alla legge sulla protezione della Costituzione del Nord Reno–Westfalia, che riconosceva la possibilità, per un'agenzia di intelligence governativa, di accedere a sistemi informatici e di monitorarli in modo occulto (art. 5, comma 2, n. 11).

Ciò che rende la pronuncia un caso unico nel panorama europeo non è tanto la conclusione a cui giunge la Corte, quanto piuttosto l'iter argomentativo seguito e che conduce a far

[19] È da segnalare che da ultimo, nel febbraio di quest'anno, il Ministro degli interni ha annunciato l'approvazione di un nuovo Trojan di Stato, che si sostanzierebbe nella intercettazione delle comunicazioni in corso, e non si estenderebbe ai contenuti e ai documenti già presenti nella memoria del dispositivo.

[20] Sentenza del Bundesverfassungsgericht del 27 febbraio 2008; per un commento alla sentenza v. R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung,* in *Riv. trim. dir. pen. eco.,* 3, 2009, 679 ss.

delineare, in virtù della pronuncia di incostituzionalità della disposizione, un nuovo diritto fondamentale[21]. La previsione di un diritto autonomo, riconosciuto in capo al cittadino/utente e posto a protezione di un suo generale diritto alla dignità[22] di fronte ai possibili usi delle tecnologie dell'informazione e della comunicazione, si è avvertito come necessario a fronte di un'insufficienza di tutela accordata nel nuovo contesto dagli artt. 10 e 13 della legge fondamentale tedesca. A questo proposito, la Corte evidenzia che il ricorso al *trojan horse* non può essere del tutto equiparato a una intercettazione di comunicazioni; inoltre, gli strumenti tecnologici permettono una raccolta a distanza di dati che non è legata necessariamente al luogo in cui si trova fisicamente il soggetto o meglio che, attraverso dispositivi mobili, la stessa azione, può essere svolta in molteplici luoghi e al di là del luogo privato che trova espressa tutela costituzionale.

Di fronte a un contesto di realtà virtuale in cui l'individuo espleta ormai la propria personalità e in cui circolano dati che possono riferirsi anche agli aspetti più riservati della propria esistenza, l'individuo/utente deve vedersi garantita una legittima aspettativa alla riservatezza di tali dati, che deve risultare protetta da qualsiasi accesso occulto. Se non può considerarsi a priori incostituzionale qualsiasi sistema di investigazione operato tramite mezzi tecnologi, tuttavia, occorre che questo sistema sia regolamentato, tenendo conto del bilanciamento tra i vari interessi che possono venire a scontrarsi. Da ciò deriva, per la Corte, la necessità che il legislatore rispetti il principio di chiarezza, di sufficiente determinatezza della fattispecie e il principio di proporzionalità[23]. Alla luce di quest'ultimo, in particolare, l'accesso e il monitoraggio occulto possono avere luogo solo se rispondono alla necessità di proteggere interessi e diritti predominanti come quello alla vita, alla incolumità fisica o alla libertà degli individui. Nel caso di specie, la Corte tedesca rileva che i principi individuati dalla Corte come alla base di qualsiasi intervento normativo sull'accesso a un contesto informatico – ossia, come accennato, chiarezza, determinatezza e proporzionalità - non sono rispettati

[21] In questo senso M. TORRE, *Il virus di Stato nel diritto vivente tra esigenze investigative e tutela dei diritti fondamentali,* in *Dir. pen, proc*., 2015, n. 9, p. 1169.
[22] Il diritto viene infatti fatto derivare dall'art. 1.1 della GG secondo il quale «la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla.».
[23] M. TORRE, *cit.*, p. 1170.

dall'art. 11, comma 2, par. 5, della legge sulla protezione della Costituzione del Nord Reno–Westfalia; di qui la dichiarazione di incostituzionalità di detta norma.

Di qualche mese fa è un altro intervento della Corte costituzionale tedesca, sempre in materia di intercettazioni occulte tramite utilizzo di captatori informatici[24]. In quest'ultima pronuncia, sono state dichiarate incostituzionali alcune disposizioni della legge federale denominata *Bundeskriminalmtgesetz*, che disciplina poteri e compiti della polizia federale nell'ambito della lotta al terrorismo. La premessa da cui muove la Corte va nel senso di riconoscere in capo al legislatore il compito di effettuare un bilanciamento tra la protezione che lo Stato deve accordare ai cittadini - soprattutto di fronte a minacce come quella del terrorismo internazionale - e i diritti fondamentali vantati dagli stessi, tra cui quelli alla riservatezza, alla segretezza delle comunicazioni, alla inviolabilità del domicilio. Tale bilanciamento deve essere svolto, ribadisce il *Bundesverfassungsgericht* alla luce del principio di proporzionalità.

Ora, al di là delle motivazione specifiche addotte dalla Corte e dalle singole disposizioni di legge intaccate dalla pronuncia di incostituzionalità, la sentenza appare di grande interesse in questa sede essenzialmente per due ordini di motivi[25]. Innanzitutto, perché rappresenta un importante intervento chiarificatore nel dibattito sul conflitto tra necessità dei Governi di assicurare la sicurezza nazionale e diritto dei cittadini al rispetto della propria privacy, da intendere sia nel senso di salvaguardia della riservatezza da possibili ingerenze esterne, sia come protezione dei dati personali. In secondo luogo, la pronuncia è interessante perché arriva quasi contemporaneamente – pur nella diversità delle argomentazioni e delle conclusioni cui approda - alla sentenza delle Sezioni Unite della Corte di Cassazione italiana, finendo in questo modo per ribadire, con maggiore enfasi, l'attualità di tale tema e la necessità che sia affrontato al più presto in sede legislativa.

[24] Si tratta della Sentenza Bundesverfaussungsgericht, I Senato, 20 aprile 2016, 1 BVR 966/09, 1 BVR 1140/09; un commento alla vicenda si ritrova in L. GIORDANO - A. VENEGONI, *La Corte costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici,* in *www.penalecontemporaneo.it,* 8 maggio 2016.

[25] V. in tal senso L. GIORDANO – A. VENEGONI, *cit.*.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

4. Conclusioni

A conferma dell'estrema attualità delle questioni sin qui delineate, è interessante notare come, sempre il 28 aprile 2016, la questione dell'hacking di Stato si è inserita vivacemente anche nel dibattito oltreoceano. La Corte Suprema degli USA, in virtù della sezione 2075 del titolo 28 dello *United States Code*[26], ha inviato ai Presidenti del Congresso alcuni emendamenti al *Federal Rules of Criminal Procedure*, tra cui, in particolare, la modifica alla *Rule* 41 in materia di perquisizioni e sequestri, norma che regola quando e in quali circostanze i giudici possono approvare un mandato di sequestro. La versione ad oggi in vigore della *Rule* 41 prevede la possibilità per i giudici di autorizzare operazioni di Hacking (definite dall' FBI "network investigative tecnique" cioè tecniche investigative di rete) solo nell'ambito delle loro giurisdizioni. Alla luce delle modifiche proposte, si prevede la possibilità per gli ufficiali di polizia giudiziaria e i pubblici ministeri federali di accedere da remoto a dispositivi elettronici allo scopo di effettuare perquisizione, sequestro o copia dei dati memorizzati; il decreto di autorizzazione potrà pervenire da qualsiasi giudice distrettuale, che tra l'altro potrà andare oltre la propria formale giurisdizione territoriale nel caso in cui non si sia a conoscenza della posizione fisica del mezzo da intercettare o ancora - all'interno di indagini per frode informatica - quando i computer coinvolti nell'illecito abbiano subito danneggiamenti senza autorizzazione e si trovino fisicamente in cinque o più distretti. La parola spetta ora al Congresso che, secondo quanto disposto dalla legge, avrà tempo fino al 1 dicembre per poter intervenire sul punto. In caso contrario, la norma entrerà automaticamente in vigore. In questo modo, si aprirebbe la strada a un'espansione di poteri in capo ad autorità come l'FBI, la quale si vedrebbe riconosciuta la possibilità di una intrusione legale nei computer, una volta ottenuta l'autorizzazione da parte di qualsiasi giudice negli Stati Uniti. Sul punto, non sono

[26] La sezione 2075 del titolo 28 dello *United States Code* prevede che: «The Supreme Court shall have the power to prescribe by general rules, the forms of process, writs, pleadings, and motions, and the practice and procedure in cases under title 11. Such rules shall not abridge, enlarge, or modify any substantive right. The Supreme Court shall transmit to Congress not later than May 1 of the year in which a rule prescribed under this section is to become effective a copy of the proposed rule. The rule shall take effect no earlier than December 1 of the year in which it is transmitted to Congress unless otherwise provided by law. The bankruptcy rules promulgated under this section shall prescribe a form for the statement required under section 707(b)(2)(C) of title 11 and may provide general rules on the content of such statement.» ; in definitiva si riconosce alla Corte Suprema il potere di adottare atti legislativi in merito alle regole di procedura penale a patto che non si vada ad inficiare con diritti sostanziali.

mancate critiche soprattutto alla luce dell'interferenza che tali previsioni possono provocare nei confronti del IV emendamento[27].

L'analisi fin qui svolta ha condotto a delineare un contesto di grande incertezza che, come già ribadito nel corso della trattazione, è innanzitutto da rinvenire nella mancanza di un quadro normativo in grado di dare riconoscimento a tali strumenti e di fornire tutele di fronte alle potenzialità offerte oggi dalla tecnologia.

Il giudice si è trovato di volta in volta a decidere in merito alla legittimità di nuovi mezzi di indagine di fronte a un quadro normativo invariato. In questo ruolo ha dovuto, inoltre, fare i conti con la necessità di tenere in considerazione la contrapposizione tra due diverse esigenze: da un lato quella di svolgere attività investigative, sfruttando al massimo anche le potenzialità offerte dalla tecnologia, e dall'altro quella di continuare a garantire adeguata tutela alle libertà e ai diritti dell'individuo.

Il dibattito è più che mai attuale ed è reso ancor più complesso da almeno due circostanze. La prima è l'importanza che il contesto online rappresenta oggi per ciascun individuo, come luogo di svolgimento della sua personalità e al tempo stesso come amplificatore di abusi e illeciti. La seconda circostanza attiene al contesto politico-giuridico che si è venuto a delineare, sia con gli attentati terroristici, a partire da quello dell'11 settembre, sia con lo scandalo creato dalle rivelazioni di Edward Snowden e il venire alla luce di un sistema di sorveglianza di massa che può dirsi figlio proprio di questo clima di terrore.

In tale contesto, la tecnologia ha offerto strumenti sempre più sofisticati che, se da un lato finiscono per essere non solo necessari, ma anche indispensabili nella lotta al terrorismo e alla criminalità, dall'altro finiscono per intaccare i diritti fondamentali degli individui, primo fra tutti il diritto alla riservatezza e alla protezione dei dati personali. Ancora una volta, il rischio è di rimanere implicati nel difficile equilibrio tra sicurezza nazionale e diritto alla privacy di ciascun individuo, senza fornire adeguata tutela a nessuno dei due interessi in gioco.

Ora**,** al di là delle diverse posizioni che la giurisprudenza ha espresso nel corso degli anni circa il ricorso a simili strumenti di intercettazione, ciò che si evince è la necessità, di fronte

[27] In particolare critiche sono giunte dall'*Open Technology Institute,* istituito impegnato nella promozione di iniziative per la libertà e la giustizia sociale nell'era digitale, di cui fanno parte alcuni OTP tra cui Google, Facebook, Yahooh, Netflix; sul punto v. il comunicato stampa dell'OTI disponibile a questo indirizzo https://www.newamerica.org/oti/oti-to-congress-block-new-government-hacking-proposal-2/.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

alle nuove frontiere tecniche del digitale, di dare una risposta di tipo legislativo al fine di giungere il prima possibile a una disciplina che definisca in maniera più chiara l'ammissibilità e i limiti di applicazione di tali strumenti.