ALESSANDRA TESTAGUZZA

Exitus acta probat
"Trojan" di Stato: la composizione di un conflitto

1. La questione

Se ne sente parlare da parecchio tempo ormai, ma si è dovuto attendere fino al 28 aprile u.s. per avere un giudizio definitivo dal giudice della nomofilachia sulla utilizzabilità dei risultati acquisiti tramite il c.d. "*virus* auto-istallante". Chiamate a raccolta dall'ordinanza di rimessione della sesta Sezione[1], le Sezioni unite hanno dovuto stabilire se anche nei luoghi di privata dimora *ex* art. 614 c.p., pure non singolarmente individuati e anche se *ivi* non si stia svolgendo l'attività criminosa – sia consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un "captatore informatico" in dispositivi elettronici portatili (ad es., *personal computer, tablet, smartphone* ecc.).

Una decisione destinata ad avere senz'altro largo eco in dottrina per i risultati a cui è pervenuta e che – come si avrà modo di appurare meglio nel prosieguo - apre (seppur parzialmente) ad un utilizzo disinibito dell'"intruso informatico", specie nella delicata fase delle indagini. Per comprendere appieno la portata del *dictum* di legittimità, tuttavia, è opportuno da un lato chiarire *l'ubi consistam* del captatore e, dall'altro, individuare le principali problematicità ad esso contigue sì da verificare, a conclusione di un percorso irto di contraddizioni ed in perenne bilico fra istanze di prevenzione e garanzie di riservatezza, se sia doveroso (o quantomeno conveniente) un intervento *ad hoc* del Legislatore che scongiuri il rischio di un (già da tempo avvertito) "assolutismo giudiziario ed investigativo".

2.Il controverso "Trojan": fra veti ed aperture

Diversi i nomi utilizzati: generalmente si parla di captatore informatico, di agente intrusore, o di *virus* autoinstallante ma anche di *trojan* o *spyware*. Dal punto di vista tecnico si tratta di *software* malevoli in grado di infettare un dispositivo (smartphone, tablet o pc), di accedere a tutta la sua attività (comunicazioni telefoniche, mail, chat, foto, Skype, navigazione web, file) e di attivare, da remoto, microfono e videocamere. La loro funzione è ben nota agli organi inquirenti (un po' meno ai consociati, informati della esistenza di strumenti di tal fatta dai soli organi di stampa e con cadenza tutt'altro che regolare): agevo-

[1] Cass., Sez. VI,. 10 marzo 2016, Scurato, in *Mass. Uff.,* n. 13884.

lare le indagini e la ricerca di indizi nei procedimenti di maggior allarme sociale ricorrendo ai captatori nella loro veste "intercettiva", specie nei casi di cui al co. 2 dell'art. 266 c.p.p. (anche se in assenza delle condizioni ivi prescritte). Ciò basta a rendere pressoché inevitabile la contrazione di quel diritto alla riservatezza che la normativa interna – supportata dalla granitica giurisprudenza sovranazionale – tende a presidiare. Ma a destare perplessità non sembra essere soltanto il potenziale uso spregiudicato di un mezzo idoneo a consentire l'acquisto, da parte di soggetti terzi, del pieno controllo del dispositivo elettronico "ospitante", quanto piuttosto la mancata definizione normativa di procedure o protocolli vincolanti tali da rendere controllabile *ex post* l'operato stesso degli investigatori.

La latitanza del Legislatore in *subiecta materia*, infatti, pone una serie di interrogativi cui con difficoltà e, ad oggi solo in via pretoria, si è tentato di dare risposta. Si pensi alla definizione delle competenze fra uffici delle Procure (quali di essi, per esempio, in relazione ad indagini collegate *ex* art. 371 c.p.p., siano legittimati all'utilizzo del "*trojan*", ovvero se tutti debbano ritenersi a ciò autorizzati in considerazione della richiamata possibilità di procedere, congiuntamente, al compimento di specifici atti); alla definizione dei limiti oltre i quali il ricorso ai captatori debba ritenersi abusivo; alla individuazione dei soggetti chiamati a verificarne il rispetto; alle sanzioni processuali prospettabili (inutilizzabilità di quanto captato?); ai tempi di conservazione dei file; al destino riservato a quelle informazioni causalmente acquisite ma non inerenti l'indagine in corso; ai casi in cui il computer intercettato sia in uso a due diversi soggetti (non tutti sottoposti ad indagine), ciascuno in grado di farvi accesso con proprie credenziali; ai casi di concorso di reati e così via. Si tratta, in sostanza, di delimitare quei presupposti oggettivi e soggettivi vigenti attualmente per le intercettazioni tradizionali e che – a rigore- dovrebbero pacificamente ammettersi per gli strumenti dotati di una maggior pervasività ed incidenza, soprattutto nella dimensione costituzionale.

Va oltretutto rammentato che, ad oggi, quando una procura autorizza una captazione, si rivolge ad un operatore privato i cui requisiti di integrità e serietà nella conduzione delle relative attività – stante l'assenza di protocolli *ad hoc* da imporre a pena di invalidazione di quanto compiuto – vengono spesso supposti per esistenti attraverso un'accettazione fideistica dei risultati dallo stesso confezionati *inaudita altera parte* e che sfuggono, pertanto, a qualsivoglia forma di controllo difensivo.

In passato la questione era stata affrontata dalla ben conosciuta sentenza Virruso[2] e poi nel noto "caso Bisignani", ma l'interpretazione che se ne era allora offerta si limitava a conferire legittimazione indiretta ai mezzi atipici di ricerca della prova, pur avendo risolto il problema non tanto dalla prospettiva dello strumento di "cattura" utilizzato, quanto dal legittimo ingresso nel processo dell'elemento probatorio così raccolto, ai sensi dell'art. 189 c.p.p[3].
All'epoca, il ruolo del captatore appariva circoscritto alla mera apprensione del flusso unidirezionale di informazioni (presenti e future) veicolato dall'utilizzatore sul proprio computer attraverso i comuni software di videoscrittura, non anche alla acquisizione del relativo contenuto comunicativo. Il ché aveva da un lato indotto parte della dottrina ad escludere il richiamo alle garanzie apprestate dall'art. 15 Cost. a tutela della segretezza delle comunicazioni ma dall'altro fatto sorgere (mai sopiti) dubbi intorno alla scelta di privilegiare l'ubicazione materiale del sistema informatico piuttosto che la sua dimensione astratta, quale proiezione di un luogo, ascrivendo rilevanza alla prima anziché alla seconda ed entrando così in conflitto con il concetto stesso di domicilio informatico inteso quale spazio ideale - ma anche fisico - in cui sono contenuti i dati informatici di pertinenza della persona[4].
Il suo diverso e più esteso ambito cognitivo, tuttavia, ha inevitabilmente accentuato la sensibilità valutativa della giurisprudenza di legittimità la quale, nel recente passato[5], chiamata a pronunciarsi sull'uso incontrollato del captatore integrato in un apparecchio mobile - per natura non sottoponibile a restrizioni spaziali ovvero temporali e dunque suscettibile di trasformarsi in una vera e propria "spia" ambientale (nel caso di specie si trattava di uno smartphone) - ha ritenuto, con fare prudente, che "una corretta ermeneutica della norma di cui all'art. 15 Cost. osta all'attribuzione, al disposto dell'art. 266 c.p.p., comma 2, di una latitudine operativa così ampia da ricomprendere intercettazioni ambientali effettuate in qualunque luogo. La norma costituzionale pone infatti il fondamentale principio secondo il quale la libertà e la segretezza delle comunicazioni sono inviolabili, ammettendo una limitazione soltanto per atto motivato dell'autorità giudiziaria e con le garanzie stabilite dalla legge. Ne deriva che le norme che prevedono la possibilità di intercettare comunicazioni tra presenti sono di stretta interpretazione, ragion per cui non può considerarsi giuridicamente corretto attribuire alla norma codicistica una portata ap-

[2] Cass., Sez. V, 14 ottobre 2009, Virruso, in *Mass. Uff.,* n. 246955.
[3] BATTINIERI, *La perquisizione online. Tra esigenze investigative e ricerca atipica della prova*, in *Sic. e giust.*, 2012, 45.
[4] Cass., Sez. V, 26 ottobre 2012, non massimata
[5] Cass., Sez. VI, 26 maggio 2015, Musumeci, in *questa Rivista* online.

plicativa così ampia da includere la possibilità di una captazione esperibile ovunque il soggetto si sposti. Viceversa, l'unica opzione interpretativa compatibile con il dettato costituzionale è quella secondo la quale l'intercettazione ambientale deve avvenire in luoghi ben circoscritti e individuati ab origine e non in qualunque luogo si trovi il soggetto. Tant'è che, in giurisprudenza, si ammette la variazione dei luoghi in cui deve svolgersi la captazione solo se rientrante nella specificità dell'ambiente oggetto dell'intercettazione autorizzata[6]". In altri termini, per la sesta Sezione, si tratterebbe 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. Dunque, in assenza della specificazione dei luoghi in cui effettuare l'intercettazione ambientale, la Corte opta per l'illegittimità e la conseguente inutilizzabilità delle stesse non essendo consentita *ad libitum* l'effettuazione di intercettazioni tra presenti.

Eppure a smorzare i toni del vivace dibattito è intervenuta l'ordinanza di rimessione n. 113884 del 10 marzo scorso (sempre a firma della sesta Sezione) con la quale si è tentato un approccio revisionista in materia, ben lontano da quella ortodossia giuridica fino a poco tempo prima condivisa. Il ragionamento del Collegio parte, infatti, con il rilevare che la pretesa di anticipata e precisa indicazione dei luoghi interessati dall'attività captativa sia *ex se* incompatibile – per ragioni tecniche – con lo specifico tipo di intercettazione compiuta in quanto saldamente ancorata al dispositivo elettronico di riferimento, sia esso *smartphone*, *tablet* ovvero computer portatile e, dunque, itinerante. Ciò comporta l'oggettiva impossibilità per il giudice di conoscere preventivamente gli spostamenti della persona che abbia in uso il dispositivo elettronico sottoposto ad intercettazione e la conseguente incapacità di dare indicazioni sui luoghi.

Riconosciuta la collocazione di tali tecniche investigative nell'ambito della disciplina dell'art. 266, co. 2, c.p.p., per gli ermellini, ciò che rileva è che il decreto autorizzativo sia adeguatamente motivato per giustificare le ragioni per

[6] Cass., Sez. VI, 11 dicembre 2007, Sitzia, in *Mass. Uff.,* n. 239634; Id., Sez. V, 6 ottobre 2011, Ciancitto, in *Mass. Uff.* n. 25237; Id., Sez. II, 15 dicembre 2010, Fontana, in *Mass. Uff.* n. 249207; Cass., Sez. II, 8 aprile 2014, Alvaro, *Mass. Uff.*, n. 259256.

le quali si ritiene debba utilizzarsi la metodica dell'installazione da remoto, consentendo così una captazione dinamica.
Aggiungendo che allorquando si ammetta la possibilità di utilizzare l'intercettazione per virus informatico, in mancanza della possibilità concreta di sospensione o interruzione della registrazione, il controllo non potrà che essere successivo e riguardare il regime dell'inutilizzabilità delle conversazioni captate in uno dei luoghi indicati dall'art. 614 c.p.
Tuttavia, a fronte di intercettazioni tra presenti relative a procedimenti di criminalità organizzata, disposte ai sensi dell'art. 13 d.l. 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203 e consentite anche laddove non vi sia motivo di ritenere che nei luoghi indicati dall'art. 614 c.p. si stia svolgendo l'attività criminosa, l'individuazione del luogo risulta ancor più irrilevante, anche in rapporto all'utilizzo della tecnica del *virus* informatico stante l'assenza di una apposita disciplina in deroga.
Considerata, dunque, la delicatezza della materia, in cui il ricorso a strumenti di sofisticata tecnica informatica, di così formidabile invadenza nella sfera della privacy e nello stesso tempo di applicazione tendenzialmente semplice, può determinare, da un lato, la compromissione di diritti costituzionali, dall'altro, assicurare una maggiore capacità investigativa finalizzata alla repressione di gravi reati, il Collegio ha ritenuto opportuno rimettere la questione alle Sezioni unite, formulando tre diverse questioni per evitare potenziali contrasti di giurisprudenza anche (e soprattutto) tenuto conto della ormai diffusa utilizzazione dell' "agente intrusore". In particolare, si è chiesto:
– se il decreto che dispone l'intercettazione di conversazioni o comunicazioni attraverso l'installazione in congegni elettronici di un virus informatico debba indicare, a pena di inutilizzabilità dei relativi risultati, i luoghi ove deve avvenire la relativa captazione;
– se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, co. 2, c.p.p.;
– se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.

3. La decisione delle Sezioni Unite

La pronuncia non si è fatta attendere e ha optato per una soluzione favorevole all'utilizzo del captatore limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica (a norma dell'art. 13 d.l. n. 152 del 1991), intendendosi per tali quelli elencati nell'art. 51, co. 3-*bis* e 3-*quater*,

c.p.p., nonché quelli comunque facenti capo a un'associazione per delinquere, con esclusione del mero concorso di persone nel reato.
Sembra, dunque, particolarmente avvertita l'esigenza di contrasto a fenomeni largamente in crescita – criminalità organizzata e attività terroristiche su tutti – per i quali, oltretutto, a distanza di poco più di un anno si è agito con un decreto *ad hoc* (d.l. 7 del 2015 convertito in legge 13 aprile 2015, n. 43).
A far cadere il precedente contrario della Cassazione del 2015 (sentenza n. 27100), che escludeva l'utilizzabilità come prova delle captazioni mediante virus informatico in mancanza di una preventiva indicazione dei luoghi da parte del giudice, le Sezioni unite richiamano l'articolo 13 del decreto antimafia del 1991 (n. 152), convertito con modificazioni dalla l. 12 luglio 1991, n. 203, ai sensi del quale "quando si tratta di intercettazione di comunicazioni tra presenti disposta in un procedimento relativo a un delitto di criminalità organizzata e che avvenga nei luoghi indicati dall'art. 614 del codice penale, l'intercettazione è consentita anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa. È la gravità dei reati per i quali si procede, infatti, che giustifica la deroga al regime ordinario previsto dagli artt. 266 e ss c.p.p. e che, in talune circostante, consente altresì il ricorso a strumenti preventivi ulteriori, quali quelli indicati dall'art. 226 disp. att. c.p.p.
I dubbi di legittimità costituzionale che sembrano, *prima facie*, profilarsi sono tutti incentrati sulla natura vagamente camaleontica dello strumento utilizzato, che solo riduttivamente potrebbe essere qualificato come microspia d'avanguardia. Il ruolo dallo stesso assolto, infatti, è ben più articolato ed esaustivo – in termini di acquisizione di elementi utili alle indagini – rispetto a quanto potrebbe ricavarsi dalla installazione di una classica "cimice" o "videocamera nascosta". E se queste ultime scontano il limite di un immobilismo "statico", ascrivibile alla loro stessa natura– le prime trovano, al contrario, conforto in un vero e proprio immobilismo "dinamico", itinerante, riconducibile non tanto (*rectius* non solo) all'oggetto di riferimento quanto piuttosto alla persona stessa attenzionata dagli inquirenti. Appropriarsi del contenuto di *computer*, *smartphone* e *tablet* equivale, del resto, ad assumere il pieno controllo dei principali momenti di vita dell'indagato. Così non è mancato chi, considerandoli vere e proprie "pertinenze domiciliari" – in ciò rievocando l'accezione civilistica di cui all'art. 817 c.c. [7] - ha ritenuto che l'assenza di una normativa *ad hoc* in materia possa difficilmente coniugarsi con le garanzie e

[7] La norma recita al co. I "Sono pertinenze le cose destinate in modo durevole a servizio o ad ornamento di un'altra cosa". Per la giurisprudenza la destinazione deve essere caratterizzata dal requisito della durevolezza, intesa nel senso che, pur non essendo necessarie la perpetuità e la permanenza, il rapporto pertinenziale non può essere né occasionale né temporaneo.

con i diritti assicurati dal testo costituzionale agli artt. 14 e 15 Cost. e come tali insuscettibili di essere obliterati *per saltum.*
Il Collegio, tuttavia, non pare condividere tali preoccupazioni probabilmente consolato da quegli esiti pretori provenienti da Strasburgo in virtù dei quali, in tema di intercettazioni telefoniche ed ambientali, il parametro di riferimento deve essere l'art. 8 della Convenzione. Più nello specifico: affinché le procedure condotte in uno Stato membro non si pongano con essa in contrasto, occorre innanzitutto che l'ingerenza nella "vita privata" sia prevista per legge, sia necessaria in una società democratica e che la legge persegua fini legittimi, indicati nel paragrafo 2 dell'art. 8 CEDU. L'ingerenza dell'Autorità pubblica viene infatti condizionata alla sussistenza di esigenze connesse alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui". Prerogative facilmente individuabili nei delitti di criminalità organizzata elencati dagli artt. 51 co. 3- *bis* e 3- *quater* c.p.p.
Va dato atto che, in difetto di una definizione normativa interna, la Corte richiama la nozione di criminalità adottata dalla decisione quadro 2008/841/GAI del Consiglio dell'Unione del 24 ottobre 2008 (relativa alla lotta contro la criminalità organizzata) secondo la quale per «organizzazione criminale» deve intendersi l'associazione strutturata di più di due persone, stabilita da tempo, che agisca in modo concertato allo scopo di commettere reati punibili con una pena privativa della libertà o con una misura di sicurezza privativa della libertà non inferiore a quattro anni o con una pena più grave per ricavarne, direttamente o indirettamente, un vantaggio finanziario o un altro vantaggio materiale; mentre per «associazione strutturata», un'associazione che non si è costituita fortuitamente per la commissione estemporanea di un reato e che non deve necessariamente prevedere ruoli formalmente definiti per i suoi membri, continuità nella composizione o una struttura articolata.
Alla luce delle suddette coordinate, pertanto, il vincolo associativo volto alla commissione dei delitti indicati dalla norma processuale, è sufficiente ad autorizzare la predisposizione di strumenti investigativi "atipici" per il sistema ma ad esso verosimilmente conformi.

4. Considerazioni finali e critiche

Come si diceva in apertura, la posizione assunta dalla Corte di legittimità è destinata inevitabilmente a suscitare critiche se non anche radicali opposizioni. Del resto, che il clima fosse rovente se ne era già avuta una avvisaglia con

la presentazione della proposta di L. n. 3740, del 2 dicembre 2015, recante Modifica all'articolo 266-*bis* del codice di procedura penale, in materia di intercettazione e di comunicazioni informatiche o telematiche" nella quale – a fronte dell'innalzamento della minaccia terroristica, in forme spesso nuove e di inusitata violenza e concepita come fattore di instabilità dell'intero quadro geo-politico – si caldeggiava l'idea di adottare, sia sul versante interno che internazionale, misure più stringenti e strategicamente efficaci nella lotta al terrorismo. Tra queste, appunto, la possibilità di consentire alle Forze di polizia l'utilizzo di nuovi programmi idonei a favorire l'accesso da remoto ai dati presenti nei sistemi informatici.

La proposta, a detta dei più, "liberticida" venne abbandonata nel clamore di chi vi intravedeva un velato (ma non troppo) ritorno al totalitarismo e ai connessi regimi inquisitori fermo poi essere riconsiderata solo dopo gli ultimi attentati di Bruxelles con il solito altalenante atteggiamento, a mezza via fra il decisionismo d'impatto e il garantismo meditativo.

La Corte oggi sembra aver rotto gli indugi, facoltizzando le procure – nei limiti di cui si è detto – all'utilizzo di questi strumenti, evidentemente consapevole della necessità di un maggior rigore nella lotta a delitti particolarmente gravi e dalle potenzialità distruttive. Nel bilanciamento degli interessi in gioco, quindi, la riservatezza cede il passo alla prevenzione, con l'avallo di una interpretazione forzosa dell'art. 13 del decreto antimafia n. 152/1991.

Il richiamo a tale norma, tuttavia, potrebbe suscitare delle riserve ove intesa quale unica base legittimante le operazioni *de quibus.* Nel consentire l'avvio delle procedure intercettive anche al di là dei limiti indicati dal secondo comma dell'art. 266 c.p.p., essa circoscrive il suo spazio applicativo ai soli delitti di criminalità organizzata, nulla accennando per le non meglio specificate ipotesi di "criminalità organizzata, *anche terroristica*", impropriamente ricondotta nei ranghi degli artt. 51 co. 3-bis e co.3-quater c.p.p.

Ferma la generale impraticabilità di un rinvio *per relationem* nelle materie "ad alto contenuto costituzionale", va qui osservato come i parametri evocati dal Collegio appaiano non del tutto collimanti con il dettato normativo il quale, lungi dal coniugare i delitti associativi (ex art. 416 c.p.) con le norme del codice penale relative alle associazioni con finalità di terrorismo (ex art. 270-bis c.p), ne evidenzia – al contrario – i tratti distintivi. Il riferimento ai delitti con finalità di terrorismo, infatti, impone una connotazione in via "principale" degli stessi, e non anche "accessoria" o meramente "qualificante", come sostenuto dal Supremo consesso.

L'assenza di una definizione normativa del concetto di criminalità organizzata e – di conseguenza – di ciò che in essa possa essere o non essere ricompreso

senz'altro offre un'occasione importante per il sub ingresso di una lettura estensiva delle disposizioni codicistiche ma corre anche il rischio di sconfinamenti arbitrari, giustificati solo da contingenze storico-temporali.
Va tuttavia rilevato che ciò che a taluni appare *prima facie* sintomatico del ripristino di uno Stato di polizia, con attribuzione di poteri incontrollati ed incontrollabili agli inquirenti, rappresenta ben poca cosa rispetto al contesto europeo: la Gran Bretagna, per esempio, con la proposta di legge sui poteri investigativi nota come IP Bill (Investigatory Powers Bill), sembra voler dare un via libera incondizionato all'*hacking* di Stato, usandolo anche su persone non direttamente indagate ma utili per ottenere informazioni su altri e appoggiandosi direttamente ai fornitori di connettività internet (Isp).
Al mutar dello scenario mutano, quindi, le risposte che lo Stato - nella veste di garante della sicurezza dei cittadini – è tenuto ad adottare supportato da una giurisprudenza che, oggi, pare esprimere un giudizio dal sapore finalisticamente orientato.
E dunque, pur consapevoli della necessità di una omologazione degli strumenti e di un processo di verifica, certificabile e documentato, posto a garanzia dei più alti valori costituzionali del sistema, cui indubbiamente lo Stato – legislatore deve farsi carico nel prossimo futuro, proprio quelle istanze di prevenzione e tutela della collettività di cui si è fatto cenno portano a ritenere che la posizione espressa in ultimo grado non possa essere passibile di censure per la sola maldestra inerzia di un Parlamento silente.
Del resto, come un celebre Autore ebbe a dire in passato, «i mezzi saranno sempre ritenuti onorevoli e da ciascuno laudati» se volti a «vincere e mantenere lo Stato[8]».

[8] MACHIAVELLI, *Il principe,* cap. XVIII.