filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

I virus informatici per scopi intercettivi nei procedimenti di criminalità organizzata: mezzi di cura o agenti patogeni?

Riflessioni su Sezioni unite penali RG 6889/2016 del 29 aprile 2016

20 Giugno 2016

Vincenzo Giglio

Premessa

Le **intercettazioni** sono da sempre un tema caldo.

Svelano reati, questo è sicuro. Ma mettono anche a nudo un mondo di segreti, tresche, reti di relazioni, piccole e grandi manie, propensioni, ideologie, simpatie e ripulse.

La gente ovviamente ne è ghiotta. Magari nessuno è disposto ad ammetterlo ma molti leggono con avida **curiosità** i resoconti di stampa che riportano ciò che le intercettazioni hanno sottratto al segreto. E più sono integrali quei resoconti, più li si reputa interessanti, più si estendono a dettagli intimi e privati, più risultano attrattivi.

Al tempo stesso, tuttavia, le intercettazioni creano un vago ma diffuso senso di **timore**. Come se ognuno potesse rimanerne vittima, a prescindere da qualunque personale collegamento con attività criminali. Capita così che non solo chi delinque ma anche persone dalla vita immacolata si costringano a un linguaggio sorvegliato o addirittura criptico, finendo per trattare i dispositivi di comunicazione come strumenti satanici.

La questione diventa spinosa se considerata nel più ampio contesto dei rapporti tra la magistratura e gli altri poteri. In questo campo, va da sé, l'ordine giudiziario gode di una situazione oggettiva di vantaggio per il solo fatto di detenere il potere intercettivo. Tutti gli altri, si intende la classe politica nel suo complesso e le istituzioni guidate dai suoi rappresentanti, si trovano invece in una condizione di handicap. Per una considerazione molto semplice: spettano alla politica non solo gli indirizzi macroeconomici del Paese ma anche, direttamente o indirettamente, le decisioni di dettaglio, quella che determinano concretamente le direzioni verso cui spingere la **spesa pubblica**.

E ovviamente, dove c'è spesa ci sono affari e interessi, non sempre e non tutti leciti. Il ceto politico è quindi fisiologicamente più vulnerabile ed esposto alla rivelazione dei suoi segreti, delle sue parole, dei suoi riti. Il che può accadere in occasione e in conseguenza della commissione di reati ma anche in contesti privi di rilievo penale. E tuttavia quei segreti, quelle parole, quei riti potrebbero non piacere anche in questo secondo caso, risultare antipatici o imbarazzanti. E potrebbero, come talvolta è successo, determinare riflessi istituzionali di non poco conto, determinare fortune o rovesci elettorali, provocare la caduta di quello e l'ascesa di quell'altro e così via.

Si spiega così perché il tema delle intercettazioni è spesso al centro del dibattito politico – istituzionale e altrettanto spesso è l'occasione di profonde divergenze ideologiche e culturali.

Questo quadro, già di per sé intricato, deve fare i conti con un ulteriore fattore che ne moltiplica la complessità. L'evoluzione scientifica sforna con velocità impressionante **nuove tecnologie** che, quando

applicate alle comunicazioni, ne consentono un controllo pressochè illimitato, al di fuori di ogni possibilità di efficace reazione da parte di chi comunica.

Non ci si inoltra nel dettaglio tecnico ma è certo che le intercettazioni disposte con la tecnologia di oggi consentono possibilità sconosciute ieri.

Aumenta l'efficienza ma, contestualmente, anche l'invasività di questo strumento investigativo fino a livelli il cui picco potrebbe andare ben oltre ciò che si considera lecito e tollerabile in una società democratica e risultare lesivo dei suoi valori fondanti.

L'occasione per riflettere su tutto questo è offerta dal recentissimo **arresto delle Sezioni unite che hanno avallato l'uso del virus informatico Trojan horse a fini intercettivi nell'ambito dei procedimenti per delitti di criminalità organizzata**.

È una decisione che farà discutere – e questo è un bene – e che provocherà immediati riflessi nelle strategie e metodiche degli uffici inquirenti e nella valutazione giudiziaria dei loro risultati.

Di sicuro chi ha il compito di accertare e perseguire i reati avrà più frecce al suo arco ma resta da vedere se questa accresciuta efficienza imporrà un prezzo in termini di riduzione della tutela della sfera di riservatezza dei consociati.

1) La questione concreta

Da qualche anno si è affacciata sulle scene investigative una modalità di intercettazione che fa leva su virus informatici del tipo Trojan horse.

Il virus viene solitamente installato da remoto inviando una e-mail o un sms al bersaglio prescelto (un personal computer, uno smartphone o un tablet), beninteso all'insaputa di chi ne fa uso.

Una volta completata l'operazione, il suo realizzatore dispone di molteplici opzioni ed in particolare: il controllo a distanza del dispositivo infettato (l'operatore può servirsene senza limiti, compiendovi ogni tipo di attività); la visualizzazione di tutte le operazioni compiute dal detentore; la visualizzazione e l'estrazione di tutti i dati contenuti nel dispositivo; la sua messa fuori uso; l'attivazione del microfono e della webcam del dispositivo e quindi la possibilità di ottenere riprese audio e video.

In sostanza, **l'operatore ha il completo controllo non solo delle attività informatiche compiute dall'utilizzatore del dispositivo ma anche dei suoi movimenti e delle sue comunicazioni**. Quasi della sua vita, si potrebbe dire.

2) I discordanti indirizzi interpretativi sull'uso di virus informatici in funzione intercettiva

Sono poche ma piuttosto significative le decisioni di legittimità che si riferiscono al tema in esame.

Un primo caso fu risolto dalla quinta sezione penale della Corte di Cassazione con la **sentenza n. 16556 del 14 ottobre 2009**.

Un PM aveva disposto l'acquisizione in copia, ai sensi dell'articolo 234 del codice di procedura penale, della documentazione informatica memorizzata all'interno del PC di un indagato. La novità stava nel fatto che l'acquisizione era stata ottenuta non, come solitamente avviene, con un decreto di sequestro ma mediante l'uso di un captatore informatico.

La difesa eccepì che, a dispetto del richiamo all'articolo 234, il PM aveva di fatto dato vita ad un'intercettazione che doveva essere considerata illegittima per difetto di autorizzazione.

La Corte di Cassazione rigettò il ricorso.

I giudici di legittimità osservarono anzitutto che "*per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici*". Il PM si era invece limitato a disporre una semplice operazione di

estrazione dati i quali avevano ad oggetto non flussi di comunicazioni ma "*una elaborazione del pensiero e la sua esternazione in scrittura su di un personal computer oppure mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato*". Si era quindi mosso nell'ambito dell'articolo 189 codice di procedura penale dando vita cioè ad una prova atipica.

Negli anni successivi le cose si complicarono, come era facilmente prevedibile.

Una volta che una tecnologia è disponibile, è chiaro che la tendenza è di utilizzarla in ogni direzione possibile e questo vale in ogni ambito, ivi compreso quello giudiziario.

Le nuove frontiere applicative sono venute più volte all'attenzione della sesta sezione penale della Corte di Cassazione e, come si vedrà, la risposta è stata tutt'altro che univoca.

Viene anzitutto in rilievo, in ordine temporale, la **sentenza n. 24237 del 2015**.

Un tale era stato destinatario di un'ordinanza custodiale in carcere in quanto gravemente indiziato del delitto ex articolo 416 bis del codice penale. Il suo difensore aveva presentato istanza di riesame al competente Tribunale con esito negativo. Fece quindi ricorso per cassazione.

I più pregnanti motivi di impugnazione facevano rilevare che i gravi indizi a carico dell'indagato erano stati ottenuti con un'intercettazione realizzata tramite un virus informatico che aveva consentito la captazione del traffico dati dei smartphone bersaglio e delle conversazioni tra presenti avvenute nel raggio d'azione di tali apparecchiature delle quali erano stati attivati da remoto il microfono e la videocamera.

Il difensore del ricorrente aveva eccepito che l'intercettazione così disposta sfuggiva per sua natura a qualsiasi restrizione spaziale e temporale e consentiva un controllo indiscriminato dell'intera vita privata dei soggetti intercettati e di coloro che gli stavano vicini.

Era ben possibile, peraltro, che l'intercettazione, secondo gli spostamenti effettuati dal destinatario, avvenisse all'interno dei luoghi abitativi o di privata dimora senza che vi si stesse svolgendo alcuna attività criminosa.

Il collegio di legittimità ha rigettato il ricorso, limitandosi ad osservare che, vertendosi in un procedimento per delitti di criminalità organizzata, l'intercettazione tra presenti nei luoghi di privata dimora e affini non richiedeva il fondato motivo che vi si stesse svolgendo un'attività criminosa.

Ben diversa è stata la risposta che la stessa sezione ha dato alla medesima questione un paio di mesi più tardi con la **sentenza n. 27100/2015**.

L'iter logico seguito dai giudici di legittimità può essere così sintetizzato:

- l'attivazione da remoto del microfono dà certamente luogo ad **un'intercettazione ambientale** (rectius, **tra presenti**);
- l'articolo 266 comma 2 codice di procedura penale che regola questa tipologia intercettiva deve essere interpretato nel senso che esso si riferisce alla captazione di conversazioni che avvengono in un determinato luogo e non dovunque; se così non fosse, risulterebbe violato l'articolo 15 della Costituzione che vieta di attribuire alle intercettazioni ambientali una latitudine così ampia da risultare indeterminata;
- la specifica tecnica intercettiva usata nel caso concreto è quindi inammissibile poiché consente la captazione in qualunque luogo si rechi l'utilizzatore dello smartphone controllato;
- l'unico modo per ricondurre a legittimità tale tecnica è allora che il **decreto autorizzativo** individui con precisione e preventivamente i luoghi nei quali è consentita la captazione;
- la logica conseguenza è che non sono utilizzabili le captazioni acquisite in luoghi diversi da quelli previamente specificati; se nessun luogo è stato indicato, nessuna captazione è utilizzabile;
- l'attivazione da remoto della videocamera dà invece vita da ad una prova atipica ex articolo 189 del codice

di procedura penale ma non può essere espletata dovunque e senza limiti; è infatti vietata (ed i suoi risultati sono inutilizzabili) se riguarda ambiti domiciliari e deve invece essere autorizzata preventivamente con decreto motivato se è in grado di violare la riservatezza personale (come avverrebbe, ad esempio, se fosse inquadrato un bagno pubblico).

Sulla base di tali presupposti interpretativi, la sesta sezione ha accolto il ricorso ed annullato l'ordinanza impugnata.

3) La rimessione degli atti alle Sezioni unite

La querelle interpretativa è proseguita anche nell'anno in corso.

La sesta sezione penale è stata nuovamente chiamata in causa e, con la **decisione n. 13884/2016**, si è pronunciata nei termini che saranno immediatamente esposti.

La questione di partenza è identica ai casi precedenti sicchè se ne omette la ripetizione.

Il collegio ha anzitutto osservato che "*con riferimento alla tecnica dell'agente intrusore la pretesa di indicare con precisione e anticipatamente i luoghi interessati dall'attività captativa è incompatibile con questo tipo di intercettazione, che per ragioni tecniche prescinde dal riferimento al luogo, in quanto è collegata al dispositivo elettronico, sia esso smartphone o tablet ovvero computer portatile, sicché l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore. Ovviamente questo comporta l'oggettiva impossibilità per il giudice di conoscere preventivamente gli spostamenti della persona che ha in uso il dispositivo elettronico sottoposto ad intercettazione e, quindi, di non poter dare indicazioni sui luoghi*".

I giudici si sono quindi chiesti se questa impossibilità e l'omessa indicazione dei luoghi che ne deriva determinino l'inutilizzabilità dei risultati dell'intercettazione.

Hanno al riguardo riconosciuto che **l'uso dell'agente intrusore dà luogo ad un'intercettazione tra presenti**.

Data questa premessa, gli è stato agevole rilevare che l'indicazione specifica del luogo assume importanza solo quando la captazione debba avvenire in abitazioni o altri luoghi privati. Non perché l'indicazione corrisponda di per se stessa a un obbligo normativo ma perché serve a delimitare i luoghi ai quali riferire la verifica dell'attualità dello svolgimento di un'attività criminosa.

Ed allora, tenendo conto del carattere itinerante della captazione svolta tramite un virus informatico e della sostanziale inesigibilità non solo dell'indicazione preventiva dei luoghi della captazione ma anche del rispetto di tale eventuale indicazione (dal momento che i luoghi dipendono esclusivamente dagli spostamenti dell'utilizzatore del dispositivo controllato), **l'unico modo per salvaguardare il precetto normativo ex articolo 266 comma 2 è quello di destinare successivamente all'inutilizzabilità, previo il loro stralcio dal compendio procedimentale, le captazioni avvenute in violazione di legge**.

Va tuttavia riconosciuto – si osserva – che **anche questo accorgimento non è esente da rischi se si considera che nel procedimento *de libertate* il giudice si pronuncia normalmente sulla base dei brogliacci predisposti dalla polizia giudiziaria nei quali non sempre è agevole distinguere il luogo in cui è avvenuta la comunicazione d'interesse**. È quindi essenziale in questa fase l'apporto della difesa.

Il problema in esame risulta comunque privo di impatto allorchè le intercettazioni siano disposte nell'ambito di un procedimento per fatti di criminalità organizzata poiché opera in questo caso l'articolo 13 del Decreto Legge 152/1991 che disancora la legittimità dell'operazione dal requisito dell'attività criminosa in corso.

Per tutte queste argomentazioni il collegio di legittimità ha ritenuto di non poter condividere la pronuncia contenuta nella sentenza n. 27100/2015.

Ha quindi ravvisato un contrasto interpretativo ed ha trasmesso gli atti alle Sezioni unite, formulando i seguenti tre quesiti:

- 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'articolo 266, comma 2, codice di procedura penale;
- 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.

4) Le argomentazioni del PG presso la Corte di Cassazione

A brevissima distanza di tempo, precisamente il 28 aprile 2016, le Sezioni unite si sono pronunciate sulla questione.

Si ritiene utile tuttavia, prima di dar conto della soluzione prescelta, riportare i passaggi salienti della **memoria depositata per l'occasione dalla Procura generale presso la Corte di Cassazione**.

Si tratta di un documento di indubbio interesse sia per l'autorevolezza della fonte che per la qualità delle argomentazioni sicchè viene naturale inserirlo tra i contenuti che meglio consentono di comprendere la questione in esame.

La prima considerazione del PG è apertamente metagiuridica.

Egli constata la straordinaria velocità dei progressi delle tecnologie della captazione e, in parallelo, di quelle volte all'elusione della captazione (fondate in massima parte sulle tecniche di criptazione).

Ne trae la convinzione che **l'impiego di virus informatici, più che al potenziamento delle intercettazioni, serve in realtà a recuperare l'efficacia perduta o compromessa delle tecniche tradizionali**.

Invita quindi le Sezioni unite ad inserire anche questa esigenza nel complesso *balance* degli interessi e dei valori in gioco.

La memoria del PG passa quindi a descrivere le caratteristiche tecniche del Trojan horse e giunge ad una particolare conclusione. Vero che questo mezzo consente una molteplicità di funzioni ma ugualmente vero che proprio questa molteplicità consente l'apposizione di limiti tecnici preventivi al suo utilizzo. La legge e il diritto hanno quindi la possibilità di regolamentarne l'uso nella direzione che gli pare più opportuna alla luce dei precetti costituzionali.

Il passaggio successivo riguarda la legittimità dell'uso di questo strumento nei procedimenti per delitti di criminalità organizzata.

Il PG si concede uno spazio definitorio e nega ogni legittimazione alla locuzione "*intercettazioni ambientali* ".

Per un questione di lessico normativo, anzitutto, non avendo mai il legislatore impiegato questa espressione, ma soprattutto perché gli preme sgomberare il campo da tutte le enfatizzazioni del concetto di ambiente connesse a quella locuzione.

In altre parole: è sbagliato in partenza qualunque ragionamento che, assumendo gli ambienti determinati come parametri ineludibili di riferimento, neghi legittimazione ad intercettazioni tra presenti che prescindano dai parametri medesimi.

La conclusione è a questo punto conseguenziale: **sbaglia la sentenza n. 27100/2015 quando, anziché rifarsi all'unica distinzione normativamente consentita** – quella tra intercettazioni tra presenti e intercettazioni tra presenti in luoghi di abitazione o privata dimora – **assume come riferimento la distinzione, priva di riscontro normativo, tra intercettazioni in ambienti predeterminati e intercettazioni prive di tale predeterminazione**.

Il secondo errore di quella decisione è di non avere attribuito alcun rilievo all'articolo 13 del Decreto Legge 152/1991 e di avere quindi omesso di considerare la sua portata derogatoria rispetto alla previsione ordinaria contenuta nell'articolo 266 comma 2 codice di procedura penale.

Queste pecche motivazionali hanno fatto sì che la sentenza citata si discostasse dalla consolidata giurisprudenza precedente che aveva richiesto l'indicazione specifica dei luoghi dell'attività intercettiva solo per le intercettazioni disposte in procedimenti ordinari.

Chiarito questo punto, il PG passa ad esaminare i peculiari problemi posti dall'uso del captatore informatico nelle intercettazioni tra presenti.

Ritiene comunque necessario ricordare che nel procedimento de quo il GIP aveva espressamente negato l'autorizzazione all'uso del captatore per l'effettuazione di videoriprese e non risulta peraltro che siano stati acquisiti i contenuti dell'apparecchio controllato.

Stando così le cose, e non venendo quindi in rilievo modalità intercettive diverse dalla semplice captazione di conversazioni tra presenti, **il PG è dell'avviso che le norme vigenti consentano senz'altro e senza alcuna eccezione le intercettazioni foniche a mezzo virus informatico nei procedimenti che si occupano di criminalità organizzata**.

Il presupposto logico è che il legislatore, attraverso la normativa del 1991, ha effettuato un adeguato bilanciamento degli interessi in campo e, per così dire, ha accettato il prezzo di consentire intercettazioni in luoghi di privata dimora o abitazione anche se non vi si stia svolgendo alcuna attività penalmente rilevante.

Il PG ha di seguito escluso che lo strumento di indagine di cui si parla confligga in qualche modo con precetti costituzionali.

Di certo, non con l'articolo 15 della Costituzione che è soddisfatto con l'emissione di un atto motivato dell'autorità giudiziaria che sia rispondente alla normativa vigente.

Ma neanche con l'articolo 14 della Costituzione alla luce dei chiarissimi principi affermati dalla Consulta nella sentenza n. 135/2002 che ha escluso l'esistenza di un divieto costituzionale assoluto alla captazione di immagini in luoghi di privata dimora e demandato al giudice il compito di stabilire quali riprese siano finalizzate alla captazione di comportamenti di tipo comunicativo.

Del pari, secondo il PG, nessuna violazione dell'articolo 8 CEDU può razionalmente derivare dall'uso dei virus informatici come mezzi di intercettazione.

Dopo un dettagliato excursus giurisprudenziale, viene richiamata in particolare la **sentenza emessa il 4 dicembre 2015 dalla Corte EDU nel caso Zakharov c. Russia** che contiene una sorta di decalogo dei requisiti necessari a rendere conformi all'articolo 8 le intercettazioni.

A giudizio del PG, la sentenza in esame menziona sì il requisito dell'indicazione dei luoghi ma lo considera come alternativo all'identificazione della persona da sorvegliare.

Tutti gli altri requisiti sono perfettamente rispettati dalla normativa italiana, anche se interpretata nel senso di consentire la tecnica intercettiva del virus informatico.

In particolare, la crescente pericolosità delle organizzazioni terroristiche fa sì che sia certamente ravvisabile la necessità della misura in una società democratica.

Il PG si è infine soffermato sull'identificazione della categoria dei delitti di criminalità organizzata indicata nel più volte citato articolo 13. Ha ravvisato la necessità che le Sezioni unite ne definiscano con chiarezza il contenuto, proponendo l'uso dell'elenco contenuto nell'articolo 407 comma 2 lettera a) codice di procedura penale.

Date queste premesse, il PG ha concluso chiedendo che le Sezioni unite affermino:

- **l'ammissibilità dell'intercettazione tramite virus informatico nei procedimenti per delitti di criminalità organizzata senza necessità di predeterminazione dei luoghi** (terzo quesito);
- **le intercettazioni svolte in luoghi di abitazione o privata dimora nell'ambito di procedimenti ordinari richiedono invece la predeterminazione degli ambienti da controllare** in quanto indispensabile prerequisito per la verifica dell'attualità dello svolgimento di un'attività criminosa (primo quesito);
- **le captazioni acquisite in luoghi privati al di fuori dei presupposti di cui all'articolo 266 comma 2 codice di procedura penale non sono inutilizzabili** poiché tale sanzione è riservata a gravi patologie degli atti procedimentali mentre nel caso di specie si tratterebbe di rimediare ad una situazione dovuta agli effetti imprevedibili e incontrollabili del decreto autorizzativo (secondo quesito);
- sarebbe quindi preferibile negare in radice ogni legittimità all'uso dei virus informatici in procedimenti ordinari.

Questa è in sintesi la visione del nostro massimo organo giudiziario requirente.

5) L'intervento chiarificatore delle Sezioni unite

Dal canto loro le Sezioni unite hanno risolto la questione, chiarendo che **anche nei luoghi di privata dimora ex articolo 614 del codice penale, pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili.**

L'intercettazione è tuttavia limitata ai procedimenti per delitti di criminalità organizzata, anche di tipo terroristico, per tali dovendosi intendere quelli elencati nell'articolo 51 commi 3 bis e 3 quater codice di procedura penale nonché gli altri "*comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato*".

La soluzione appena riportata è allo stato ricavata esclusivamente dall'informazione provvisoria diramata dalla Corte suprema, non essendo ancora disponibile la motivazione.

6) Riflessioni sulla decisione delle Sezioni unite

Gli interventi delle Sezioni unite condividono in genere tre caratteristiche essenziali.

La prima è strettamente connaturale alla funzione nomofilattica dell'organo: le sue pronunce indicano una soluzione interpretativa che, se credibile e convincente, si tramuta in diritto vivente, dirada confusione e conflitti, favorisce la prevedibilità e la condivisione delle scelte giurisdizionali.

La seconda si traduce in una sorta di warning al legislatore: le Sezioni unite intervengono quando ci sono conflitti interpretativi e questi sono generalmente dovuti a norme di significato incerto o di contenuto discutibile oppure inadeguate alle esigenze contemporanee oppure a discipline carenti o addirittura omissive.

La terza ragione è meno appariscente ma non per questo di minore importanza. Il fatto stesso che le Sezioni unite prendano in carico una questione giuridica equivale ad accendere una **spia luminosa**: la nostra

massima istanza giurisdizionale avverte che si tratta di qualcosa a cui tutti, non solo i membri della comunità giuridica, devono prestare attenzione perché è destinato ad avere riflessi non solo sui processi ma anche sulle vite dei consociati, sul modo in cui i loro diritti e doveri si compongono in un equilibrio più generale, sul livello di garanzie che l'ordinamento è disposto a riconoscere e così via.

Pare innegabile, pur con la cautela imposta dalla disponibilità di una semplice informazione provvisoria, che il pronunciamento delle Sezioni unite qui commentato presenti tutte queste caratteristiche.

Ciò detto, la soluzione prescelta – questo è già chiaro – **dà il via libera all'uso dei virus informatici allorchè si intenda ricorrere ad intercettazioni in procedimenti per delitti di criminalità organizzata**.

Questa modalità diventerà quindi – e anche questa è una facile previsione – di uso comune e massivo nelle attività investigative delle DDA.

Viene per ciò stesso colmato o almeno attenuato il gap tecnologico cui il PG ha destinato la prima considerazione della sua memoria. Se ne creeranno altri, è ovvio, ma per intanto gli organi inquirenti sono messi in condizione di usare le più avanzate tecnologie captative disponibili e il Trojan horse aggiunge legittimamente alle sue varie possibili denominazioni (programma informatico, malware, agente intrusore, captatore informatico, spyware) quella di virus di Stato.

Come sempre, l'interrogativo primario è comprendere quali saranno gli effetti, giuridici e non, che questa nuova possibilità produrrà nello scenario del nostro Paese.

6.1) Gli effetti giuridici connessi all'eventuale violazione dell'articolo 266 comma 2 codice di procedura penale.

Le Sezioni unite hanno compiuto l'attività definitoria esplicitamente richiesta dal PG, chiarendo che la qualifica di procedimenti per delitti di criminalità organizzata spetta a quelli rientranti nella previsione dei commi 3° bis e quater dell'articolo 51 codice di procedura penale e agli altri in cui si procede per reati comunque facenti capo ad un'associazione a delinquere.

La formulazione dell'ultimo inciso, pur non chiarissima, sembra comunque autorizzare l'estensione di quella qualifica a qualsiasi procedimento in cui si contesti un qualunque delitto purchè ascrivibile al programma criminoso di un'associazione a delinquere.

Spetta ovviamente al PM, per fisiologia ordinamentale, individuare e circostanziare le fattispecie di reato che ritiene più congrue al fatto sottostante.

Sicchè è una parte, sia pure pubblica ed al servizio di fini pubblici, a determinare le condizioni che consentono la particolare metodica intercettiva di cui si parla.

Basta quindi, ad esempio, che un PM iscriva nel registro delle notizie di reato un delitto ordinario aggravato ex articolo 7 Decreto Legge 152/1991 oppure compreso nel programma criminoso di un'associazione a delinquere ed ha per ciò stesso, in base al criterio fissato dalle Sezioni unite, posto le condizioni per l'uso del Trojan horse.

Occorre allora chiedersi cosa potrebbe accadere se, a posteriori, si accerti che la qualificazione delle fattispecie operata inizialmente sia erronea.

In altre parole: **che sorte avrebbero le captazioni acquisite sulla base di un decreto autorizzativo che non indica luoghi specifici e non consente quindi di verificare il fondato motivo di ritenere l'attualità di una condotta criminosa in un certo luogo**, se poi fosse giudizialmente accertato che il delitto di criminalità organizzata inizialmente ipotizzato non esisteva o che il delitto comune che si assumeva in un programma associativo non aveva invece questa caratterizzazione?

Già la sola rassegna giurisprudenziale contenuta nei paragrafi precedenti dimostra l'inesistenza di risposte univoche.

Si ricorderà che, secondo la sentenza 27100/2015, le intercettazioni tra presenti sono legittime solo se precedute da un decreto autorizzativo che individui in modo chiaro e preciso i luoghi nei quali è consentita la captazione. Sono quindi inutilizzabili, secondo questa visione, sia le captazioni acquisite in luoghi diversi da quelli predeterminati sia, a maggior ragione, quelle acquisite in assenza di qualsiasi indicazione.

Si ricorderà ugualmente che la decisione 13884/2016 ha espresso una visione assai differente.

Ha considerato infatti inesigibile in fatto, a fronte dell'uso di un agente intrusore di tipo informatico, la pretesa di un'indicazione preventiva dei luoghi interessati dall'attività captativa.

Ha però ammesso l'esistenza del rischio, collegato all'inesistenza di filtri preventivi, che siano acquisite captazioni ottenute nei luoghi ex articolo 614 del codice penale.

Ha quindi manifestato l'opinione che le medesime, nei casi in cui siano state ottenute in violazione di legge - possibilità evidentemente limitata ai procedimenti in cui non si procede per delitti di criminalità organizzata - debbano essere sanzionate con l'inutilizzabilità da dichiararsi dopo il completamento delle operazioni di intercettazione.

Va peraltro sottolineato che, proprio a questo proposito, il collegio della sesta sezione ha ritenuto di porre uno specifico quesito alle Sezioni unite, volto a chiarire se la sanzione di inutilizzabilità dovesse limitarsi alle captazioni avvenute in luoghi di privata dimora in violazione dell'articolo 266 comma 2 del codice di procedura penale.

Il provvedimento di rimessione non ha esplicitato l'alternativa ma è logico immaginare che essa dovesse consistere nell'estensione dell'inutilizzabilità a tutte le captazioni, anche se acquisite in luoghi non di privata dimora.

Sempre a questo proposito, resta da dire che il relativo parere espresso dal PG è stato nel senso di non ravvisare alcuna inutilizzabilità nella situazione ipotizzata dal giudice rimettente. Ma questa valutazione presupporrebbe logicamente che il collegio della sesta sezione si fosse pronunciato in termini dubitativi sull'individuazione dell'inutilizzabilità come sanzione adeguata, il che non è avvenuto poiché l'unico dubbio era, come si è appena visto, sulla latitudine della sanzione.

La considerazione appena esposta permette di passare immediatamente alla terza soluzione proposta, cioè appunto quella del PG.

A suo giudizio – lo si ripete – le captazioni acquisite in luoghi privati al di fuori dei presupposti di cui all'articolo 266 comma 2 del codice di procedura penale non sono inutilizzabili poiché tale sanzione dovrebbe essere riservata a gravi patologie degli atti procedimentali mentre nel caso di specie si tratterebbe di rimediare ad una situazione dovuta agli effetti imprevedibili e incontrollabili del decreto autorizzativo.

L'unico rimedio possibile è allora quello di sbarrare totalmente la strada all'uso a fini intercettivi dei virus informatici nei procedimenti ordinari.

È infine a tutt'oggi ignoto il pensiero delle Sezioni unite per quest'aspetto poiché l'informazione provvisoria non contiene alcun'indicazione utile.

Sicchè, a ragionare esclusivamente sulla base degli indirizzi emersi finora nel circuito di legittimità, sarebbero possibili due opzioni: **la prima è l'inutilizzabilità, la seconda è una sorta di self restraint dei PM che dovrebbero sempre rinunciare ad avvalersi degli agenti intrusori informatici quando intendono dar vita ad intercettazioni nei procedimenti ordinari**.

Se questa è la cornice entro cui muoversi, bisogna adesso chiedersi cosa succederebbe con ciascuna delle due opzioni.

Quanto all'inutilizzabilità, è fin troppo noto il granitico indirizzo giurisprudenziale, originato da una pronuncia delle Sezioni unite, che nega l'esistenza di qualunque forma di inutilizzabilità derivata.

Ed allora, una volta affermata l'inutilizzabilità di una certa captazione, la sanzione non precluderebbe l'uso del suo risultato come *notitia criminis* e quindi, ad esempio, come legittimo input per la richiesta di una nuova sequenza intercettiva o per altre attività investigative.

Il frutto dell'albero avvelenato non sarebbe perciò considerato avvelenato anch'esso e non sarebbe condannato alla distruzione ma rimarrebbe a disposizione degli inquirenti per gli scopi predetti.

La seconda opzione viene proposta dal suo ideatore come unica soluzione possibile ma – non sembra azzardato dirlo – non risolve alcunchè. La sua concreta efficacia è infatti strettamente connessa alla discrezionalità del PM il quale, in assenza di divieti normativi o di eventuali linee guida cogenti all'interno dell'ufficio giudiziario in cui opera, potrebbe non tenerla affatto in considerazione e comportarsi quindi in tutt'altro modo.

Ma c'è di più. La stessa opzione non offre alcuna indicazione circa l'uso che debba farsi di captazioni ottenute in violazione del disposto dell'articolo 266 comma 2.

Si perdonerà l'ovvietà ma **ciò che non è inutilizzabile e non è altrimenti invalido rimane per ciò stesso in vita**.

Sicchè – ci si chiede – che uso dovrebbero fare le parti e il giudice di elementi conoscitivi che continuano a far parte del materiale procedimentale o del fascicolo dibattimentale? Possono legittimamente ignorarlo e non farne alcun uso? Oppure sono tenuti a confrontarsi con quegli elementi e dargli un significato, quale che sia?

Domande legittime alle quali manca allo stato qualsiasi risposta. Facile prevedere che si crei, almeno per questo specifico aspetto, la **confusione che pure l'intervento delle Sezioni unite avrebbe dovuto scongiurare**.

6.2) Controllabilità dell'uso del virus informatico

Così si legge testualmente nella più volte citata memoria del PG: *"La molteplicità di funzioni dei programmi informatici di cui si discute non deve indurre a credere di essere di fronte a strumenti onnipervasivi e onnipotenti, suscettibili di dar vita ad un potere invasivo esercitabile senza limiti o in forme incontrollabili sotto il profilo tecnico o giuridico.*

Al contrario è seriamente ipotizzabile l'apposizione di limiti tecnici preventivi all'impiego dei virus informatici (ad es., inibendo a priori l'operatività di alcune delle loro molteplici funzioni acquisitive).

Inoltre, ciò che più conta in questa sede, è possibile dettare i limiti giuridici delle modalità di utilizzo dei captatori (ad es. escludendo che i programmi di on line surveillance possano essere utilizzati per effettuare videoriprese o che i programmi on line search siano impiegati per acquisire dati, al di fuori o in contrasto con le regole in tema di perquisizioni e sequestri).

Ancora una volta , dunque, come avviene del resto in altri delicatissimi campi dell'esperienza umana, sono la legge ed il diritto a fissare i confini delle possibilità offerte dalla tecnologia, commisurandole ai principi dello Stato democratico di diritto, ai diritti individuali ed alle esigenze e sensibilità della collettività".

L’opinione è chiara: non bisogna avere paura delle conquiste tecnologiche e delle loro applicazioni pratiche, perché è senz’altro possibile apporre limiti tecnici al loro uso (nel caso di specie selezionando le funzioni acquisitive indispensabili ed escludendo tutte le altre) e perché si possono porre altrettanti limiti giuridici.

Il ragionamento è rassicurante ma la situazione è davvero quella descritta dal PG?

Per farsi un’idea più precisa, può servire la storia di una società italiana, di cui si omettono i riferimenti perché non essenziali, che opera nel settore dell’information technology e che risulta l’unica produttrice del programma Trojan horse.

Il suo core business è ben descritto da Carola Frediani[1].

Questa società ha conquistato più volte l’attenzione degli organi di stampa[2].

Ed allora, volendo riassumere: un’azienda alla quale le istituzioni pubbliche italiane si rivolgono frequentemente quando intendono acquistare spyware del tipo Trojan è stata hackerata, perdendo dati di interesse strategico che potrebbero essere finiti in mani sbagliatissime; sempre quell’azienda vende prodotti della stessa specie a Stati ed agenzie i cui interessi potrebbero essere in conflitto con quello nazionale.

In Italia, peraltro, operano almeno **sette società specializzate non solo nelle intercettazioni telefoniche ma anche nel monitoraggio del traffico Internet, dei servizi di messaggistica istantanea o via sms e di tracciamento via GPS e in ulteriori e più sofisticati servizi.**

Una di esse, che ha tra l’altro collaborato professionalmente con un’importante Procura italiana, fu implicata nella rivelazione indebita di una conversazione intercettata tra un autorevole esponente politico e un alto dirigente bancario a proposito della scalata ad un primario istituto di credito[3].

Altre sono specializzate nella ***virtual humint***, cioè la creazione a fini investigativi di finti profili sui social media. Si tratta di **fittizie identità on line** che possono essere tenute in vita per anni e che consentono di infiltrarsi in gruppi e comunità che si desidera tenere sotto osservazione.

Altre ancora operano direttamente nel **campo dell’intelligence vera e propria**, cioè sono in grado di analizzare e classificare grandi quantità di dati e documenti, traendoli dal web, da forum, blog e quant’altro, e trarne conclusioni su tendenze e specifiche attività.

Altre, infine, operano in particolare nel **settore delle apparecchiature di sorveglianza sotto copertura e tracciamento.**

Prendendo a prestito le parole di Luca Rinaldi, si tratta di “*un comparto che negli ultimi anni … è cresciuto a dismisura, alimentando un esercito di controllori senza controlli. Di sicuro … il Belpaese, almeno nel settore privato, rimane uno dei più attivi a livello mondiale nello sviluppo di tecnologie e software per il monitoraggio e tracciamento di comunicazioni e spostamenti*”.

Che le cose non siano proprio rassicuranti e che non tutti condividano il senso di sicurezza manifestato dal PG, lo si ricava anche dall’iter travagliato di alcune proposte di legge in materia e dal convulso dibattito politico che le ha accompagnate.

Si pensi, ad esempio, al cosiddetto **decreto antiterrorismo**, vale a dire il Decreto Legge 7/2015 convertito nella Legge 43/2015. Nella stesura iniziale del testo era stata inserita un’aggiunta all’art. 266 bis c.p.p. tale per cui l’intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi sarebbe stata consentita “*anche attraverso l’impiego di strumenti o di programmi informatici per l’acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico*”.

La proposta non è sfuggita all’attenzione di commentatori qualificati.

Così ne ha parlato, tra gli altri, Stefano Quintarelli, deputato, informatico di professione e attuale presidente

del Comitato di indirizzo dell'Agenzia per l'Italia digitale: "*L'uso di captatori informatici (trojan, keylogger, sniffer,...) quale mezzo di ricerca delle prove da parte delle Autorità Statali (giudiziarie o di sicurezza) è controverso in tutti i paesi democratici per una ragione tecnica: con quei sistemi viene compiuta una delle operazioni più invasive che lo Stato possa fare nei confronti dei cittadini, poiché quella metodologia è contestualmente una ispezione, una perquisizione, una intercettazione di comunicazioni, una acquisizione occulta di documenti e dati anche personali; tutte attività compiute in un luogo, i sistemi informatici privati, che equivalgono al domicilio. E tutte quelle attività vengono fatte al di fuori delle regole e dei limiti dettate per ognuna di esse dal Codice di Procedura Penale*"[4].

Preoccupazioni di ugual genere sono state espresse da **Antonello Soro, attuale presidente dell'Autorità garante per la protezione dei dati personali**, secondo il quale "*perplessità suscita anche l'emendamento che ammette le intercettazioni preventive (disposte dall'autorità di pubblica sicurezza nei confronti di meri sospettati), per i reati genericamente commessi on-line o comunque con strumenti informatici. Anche in tal caso l'equilibrio tra protezione dati ed esigenze investigative sembra sbilanciato verso queste ultime*".

Il risultato di opinioni come queste è stato lo stralcio della modifica dell'articolo 266 bis che è quindi scomparsa dal testo definitivo.

E tuttavia la questione non si è chiusa lì.

Difatti, il 2 dicembre 2015 la deputata Maria Gaetana Greco ha presentato alla Camera una proposta di legge la cui relazione inizia così: "*I recenti episodi verificatisi in Europa, e più in generale nel mondo, hanno evidenziato l'innalzamento della minaccia terroristica che, presentandosi in forme spesso nuove e di inusitata violenza, costituisce una gravissima insidia per la sicurezza interna e internazionale, nonché un fattore di instabilità dell'intero quadro geo-politico. Tale contesto ha reso ormai improrogabile lo sviluppo di una capacità di risposta globale attraverso misure da adottare sia sul versante interno che su quello internazionale, anche per offrire una risposta strategicamente efficace […] Tra queste misure va senz'altro considerata la possibilità di consentire alle Forze di polizia l'utilizzo di nuovi programmi informatici che permettano l'accesso da remoto ai dati presenti in un sistema informatico al fine di contrastare preventivamente i reati di terrorismo commessi mediante l'uso di tecnologie informatiche o telematiche*".

Si ripropone in sostanza, a stretto ridosso del sanguinario attentato al Bataclan di Parigi e nel clima emotivo di quei giorni, l'uso del Trojan di Stato.

È degno di nota che la proposta sia sostanzialmente identica a quella che avrebbe dovuto essere contenuta nel decreto antiterrorismo.

Così ne parla l'avvocato e giornalista Guido Scorza[5]: "*Ora, però, l'On. Greco sembra intenzionata a riprovarci e lo fa utilizzando le stesse identiche parole, una per una, attraverso le quali, all'epoca – era il febbraio del 2015 – si sarebbe già voluto far posto al trojan di Stato tra gli strumenti di indagine a disposizione di investigatori e forze dell'ordine.*

Neppure una parola in più, neppure un principio, un paletto o un vincolo in più per scongiurare il rischio che la sacrosanta esigenza di dotare chi difende la sicurezza pubblica di efficaci strumenti di indagine scivoli in una violazione massiccia della privacy dei cittadini come, purtroppo, sta accadendo in mezza Europa proprio sulla scia dei drammatici fatti di Parigi che appaiono legati ad un rapporto di causa-effetto anche all'iniziativa dell'on. Greco".

Merita infine di essere citata, per la sua incisività, l'opinione espressa qualche anno addietro, quando ancora l'uso del Trojan a fini intercettivi era di là da venire, da Carlotta Conti: "*è indispensabile sottolineare come, al giorno d'oggi, all'interno della categoria delle prove atipiche ricadano molte insidiose violazioni della riservatezza e/o di altri diritti fondamentali. Si pensi alla questione dei numerosi virus informatici idonei a captare tutti i dati che vengono inseriti all'interno di un personal computer. Sul*

punto, la Cassazione è intervenuta nel 2010 escludendo la lesione di diritti fondamentali ed annoverando l'atto tra i mezzi atipici di ricerca della prova. Eppure siffatte attività pervengono ad un livello di aggressione della riservatezza individuale che sfiora l'inviolabilità della psiche e, forse, la questione meriterebbe una maggiore attenzione"[6].

Si potrebbe continuare ma c'è già quanto basta a farsi un'idea.

Non pare possa mettersi in dubbio che le intercettazioni in generale, e l'uso di spyware in particolare, pongano complessi problemi che hanno a che fare con l'affidabilità dell'operatore privato chiamato a compiere e gestire le operazioni tecniche necessarie e l'affidabilità della tecnologia di cui l'operatore fa uso.

Il primo punto è se, come sostiene il PG, siamo in grado di prevenire senza difficoltà quei rischi e comunque di eliminarne gli effetti negativi oppure no.

Il secondo è se l'uso di tecnologie così sofisticate, rischiose e invasive possa essere consentito da un indirizzo interpretativo, per quanto autorevole ne sia la fonte, oppure sia doveroso attendere l'intervento del legislatore.

Ancora domande, come si vede, ma il fatto stesso che sia possibile porle rende in qualche modo più precaria l'architettura della costruzione giurisprudenziale in esame.

6.3) Cosa ne pensa la Corte di Strasburgo

Come si è evidenziato in precedenza, il PG, perfettamente consapevole del rilievo che in materia deve essere riconosciuto alla previsione dell'articolo 8 CEDU, ha inteso confrontarsi con la giurisprudenza della Corte EDU di Strasburgo, unica istanza legittimata ad interpretare le norme convenzionali.

La conclusione del PG è stata di assoluta conformità alla lettera ed allo spirito dell'articolo 8 dell'interpretazione proposta alle Sezioni unite.

Il perno principale su cui si è fondata la valutazione del PG è la sentenza che la Corte EDU ha emesso il 4 dicembre 2015 nel caso Zakharov c. Russia.

È stato valorizzato in particolare il passaggio, contenuto nei punti 264 e 265 della motivazione, in cui si afferma (il testo ufficiale è in lingua inglese ma qui si usa una traduzione non ufficiale in italiano) che "*per quanto riguarda il contenuto dell'autorizzazione all'intercettazione, esso deve chiaramente identificare una persona specifica da porre sotto sorveglianza o un singolo insieme di luoghi corrispondente a quelli per i quali l'autorizzazione è stata concessa. Tale identificazione può essere fatta per mezzo di nomi, indirizzi, numeri di telefono o altre informazioni rilevanti*".

Il PG ha in sostanza sottolineato che ciò che rende legittima un'attività intercettiva è l'indicazione della persona che la subisce o, in alternativa, dei luoghi in cui sarà svolta. Il che dimostra che la predeterminazione localistica non è di per se stessa indispensabile ove si possa contare sull'identificazione del destinatario.

Vero.

Bisogna però ricordare che la Corte di Strasburgo richiede ormai da tempo il requisito della **qualità della legge in materia di intercettazioni** e, tra le condizioni necessarie perché possa parlarsi di qualità accettabile, vi è quella che consente al cittadino di comprendere esattamente quali siano l'ampiezza e i limiti del potere discrezionale dell'autorità nazionale che ha il potere di ingerenza nella sfera protetta.

Sarebbe piuttosto arduo sostenere che la vigente regolamentazione normativa italiana in materia di intercettazioni consenta ai consociati di avere ben chiaro che, andandosene a spasso con i loro smartphone o incrociando qualcun altro che fa lo stesso oppure semplicemente entrando nel raggio d'azione del microfono o della videocamera del suo dispositivo, corrano per ciò stesso il rischio che i loro movimenti, le

loro parole, i loro gesti siano suscettibili di essere immortalati per esigenze giudiziarie.
Non basta: **la CEDU e la Corte che ne è custode richiedono che l'ingerenza sia necessaria in una società democratica**. Si tratta di un requisito che, forse volutamente, è vago e generico. La sua più comune interpretazione è comunque connessa all'esigenza di un equilibrio e quindi di un'adeguata proporzionalità tra la portata dell'ingerenza nella vita privata e il fine perseguito da chi esercita quell'ingerenza. Per questa via, potrebbe essere ritenuta sproporzionata anche una legittima intercettazione se le ripercussioni da essa create nella vita del singolo appaiano sovradimensionate rispetto all'interesse collettivo.
Vale infine la pena ricordare, a chiusura ed en passant, che nel **caso Lambert c. Francia (sentenza Corte EDU del 24 agosto 1998)** fu fissato il principio secondo il quale il quale la legge deve stabilire delle garanzie sufficienti non solo per il titolare della linea telefonica intercettata ma anche per il terzo che, chiamando o chiamato da tale linea, riceva delle conseguenze dall'intercettazione della sua conversazione.
Viene da immaginare, in conclusione, che la Corte di Strasburgo, se si trovasse investita di un ricorso che in qualche modo ponesse alla sua attenzione captazioni ottenute tramite la rete a strascico degli spyware, avrebbe forse qualcosa di più da dire rispetto all'opinione del PG.

Conclusione

La questione su cui si è riflettuto è estremamente attuale il che, se concorre a renderla interessante, impedisce però di contare su opinioni consolidate e, ciò che più conta, su verifiche sul campo che chiariscano se le preoccupazioni manifestate siano fondate o piuttosto il frutto di un timore irrazionale verso il "nuovo che avanza".
Si vedrà.
Certo è che gli Stati si trovano ad affrontare minacce criminali ogni giorno più complesse e insidiose e a doversi confrontare con scenari caratterizzati da contrapposizioni ideologiche, etniche, religiose, culturali che costituiscono il terreno ideale per temibili sfide alla pace e alla sicurezza sociale.
In tutto questo le nuove conquiste scientifiche e tecniche mettono a disposizione di chiunque possibilità, lecite e illecite, altrettanto complesse e versatili e inducono quindi una domanda incessante di tecnologia e innovazione.
La cosa è in sé neutra, né giusta né sbagliata, e non può comunque essere fermata, essendo illusorio ogni tentativo di rallentare i progressi umani o di indirizzarli verso percorsi predeterminati.
Si può e si deve invece fare quanto possibile perché i nuovi saperi e le nuove tecnologie vengano usati in modo da non compromettere o sciupare i valori essenziali che tengono insieme la nostra civiltà e le danno senso.
Si può e si deve cercare il miglior equilibrio possibile tra difesa sociale e libertà dei consociati.
Sperando non tanto di indovinare tutte le scelte ma di sbagliarne il meno possibile.

[1] **C. Frediani**, articolo pubblicato il 16 settembre 2013 sull'edizione web della rivista Wired. Vi si legge che: "*Le* (sue) *origini … risalgono al 2001, quando due programmatori … scrissero **E.**, un software che faceva da "suite completa per attacchi man-in-the-middle", cioè un insieme di strumenti per sniffare password e dati, registrare conversazioni e chat, e controllare da remoto un computer target. La loro creazione piacque molto alla Questura di … che era interessata a usarlo nelle indagini. Da lì iniziò la carriera dell'azienda come venditore di Trojan a forze dell'ordine e agenzie statali di vari Paesi, cioè di malware in grado di infettare silenziosamente un computer, e da quel momento in avanti di averne pieno controllo e poterne monitorare tutta l'attività*".
[2] Nell'edizione del 3 novembre 2015 di Repubblica.it Tecnologia si è data notizia di una perquisizione

disposta da una Procura nei confronti di un'azienda sulla base del sospetto che i suoi gestori, in passato dipendenti della società prima menzionata, potessero essere coinvolti in un'azione di hackeraggio a danno di quest'ultima con la violazione di 400 gigabyte di dati riservati. L'ipotesi è che gli indagati si fossero impadroniti del codice sorgente dello spyware G., cioè il programma che la società fornisce a governi e forze dell'ordine, e lo abbiano poi ceduto ad una società saudita che potrebbe a sua volta averlo trasmesso a gruppi jihadisti.

Ancora più di recente la medesima società è stata nuovamente menzionata in un articolo di cronaca, curato anch'esso da Carola Frediani ma questa volta per l'edizione web di La Stampa Tecnologia del 7 aprile 2016.

La notizia è che il 31 marzo 2016 il Ministero dello sviluppo economico ha revocato l'autorizzazione all'export di cui godeva la società in direzione dei Paesi extra UE. Secondo l'articolista, la ragione del provvedimento sarebbe in qualche modo collegata al caso di Giulio Regeni ed al fatto che l'Egitto sarebbe tra i clienti della società medesima, assieme a numerosi altri Stati africani ed asiatici.

Vengono citate due interrogazioni parlamentari nelle quali si assume che essa avrebbe venduto i suoi spyware all'intelligence egiziana.

[3] **Luca Rinaldi**, articolo pubblicato sull'edizione web di Wired.it del 16 luglio 2015.

[4] La dichiarazione è riportata da **Michele Nasi** in un articolo pubblicato sull'edizione de IlSoftware.it del 27 marzo 2015.

[5] **G. Scorza**, articolo apparso sull'edizione web de Il Fatto quotidiano del 26 gennaio 2016.

[6] **C. Conti**: *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali* (relazione tenuta ad un incontro di formazione svoltosi il 13 dicembre 2012 presso la Corte di Cassazione)".

Premessa

Le **intercettazioni** sono da sempre un tema caldo.

Svelano reati, questo è sicuro. Ma mettono anche a nudo un mondo di segreti, tresche, reti di relazioni, piccole e grandi manie, propensioni, ideologie, simpatie e ripulse.

La gente ovviamente ne è ghiotta. Magari nessuno è disposto ad ammetterlo ma molti leggono con avida **curiosità** i resoconti di stampa che riportano ciò che le intercettazioni hanno sottratto al segreto. E più sono integrali quei resoconti, più li si reputa interessanti, più si estendono a dettagli intimi e privati, più risultano attrattivi.

Al tempo stesso, tuttavia, le intercettazioni creano un vago ma diffuso senso di **timore**. Come se ognuno potesse rimanerne vittima, a prescindere da qualunque personale collegamento con attività criminali. Capita così che non solo chi delinque ma anche persone dalla vita immacolata si costringano a un linguaggio sorvegliato o addirittura criptico, finendo per trattare i dispositivi di comunicazione come strumenti satanici.

La questione diventa spinosa se considerata nel più ampio contesto dei rapporti tra la magistratura e gli altri poteri. In questo campo, va da sé, l'ordine giudiziario gode di una situazione oggettiva di vantaggio per il solo fatto di detenere il potere intercettivo. Tutti gli altri, si intende la classe politica nel suo complesso e le istituzioni guidate dai suoi rappresentanti, si trovano invece in una condizione di handicap. Per una considerazione molto semplice: spettano alla politica non solo gli indirizzi macroeconomici del Paese ma anche, direttamente o indirettamente, le decisioni di dettaglio, quella che determinano concretamente le direzioni verso cui spingere la **spesa pubblica**.

E ovviamente, dove c'è spesa ci sono affari e interessi, non sempre e non tutti leciti. Il ceto politico è

quindi fisiologicamente più vulnerabile ed esposto alla rivelazione dei suoi segreti, delle sue parole, dei suoi riti. Il che può accadere in occasione e in conseguenza della commissione di reati ma anche in contesti privi di rilievo penale. E tuttavia quei segreti, quelle parole, quei riti potrebbero non piacere anche in questo secondo caso, risultare antipatici o imbarazzanti. E potrebbero, come talvolta è successo, determinare riflessi istituzionali di non poco conto, determinare fortune o rovesci elettorali, provocare la caduta di quello e l'ascesa di quell'altro e così via.

Si spiega così perché il tema delle intercettazioni è spesso al centro del dibattito politico – istituzionale e altrettanto spesso è l'occasione di profonde divergenze ideologiche e culturali.

Questo quadro, già di per sé intricato, deve fare i conti con un ulteriore fattore che ne moltiplica la complessità. L'evoluzione scientifica sforna con velocità impressionante **nuove tecnologie** che, quando applicate alle comunicazioni, ne consentono un controllo pressochè illimitato, al di fuori di ogni possibilità di efficace reazione da parte di chi comunica.

Non ci si inoltra nel dettaglio tecnico ma è certo che le intercettazioni disposte con la tecnologia di oggi consentono possibilità sconosciute ieri.

Aumenta l'efficienza ma, contestualmente, anche l'invasività di questo strumento investigativo fino a livelli il cui picco potrebbe andare ben oltre ciò che si considera lecito e tollerabile in una società democratica e risultare lesivo dei suoi valori fondanti.

L'occasione per riflettere su tutto questo è offerta dal recentissimo **arresto delle Sezioni unite che hanno avallato l'uso del virus informatico Trojan horse a fini intercettivi nell'ambito dei procedimenti per delitti di criminalità organizzata**.

È una decisione che farà discutere – e questo è un bene – e che provocherà immediati riflessi nelle strategie e metodiche degli uffici inquirenti e nella valutazione giudiziaria dei loro risultati.

Di sicuro chi ha il compito di accertare e perseguire i reati avrà più frecce al suo arco ma resta da vedere se questa accresciuta efficienza imporrà un prezzo in termini di riduzione della tutela della sfera di riservatezza dei consociati.

1) La questione concreta

Da qualche anno si è affacciata sulle scene investigative una modalità di intercettazione che fa leva su virus informatici del tipo Trojan horse.

Il virus viene solitamente installato da remoto inviando una e-mail o un sms al bersaglio prescelto (un personal computer, uno smartphone o un tablet), beninteso all'insaputa di chi ne fa uso.

Una volta completata l'operazione, il suo realizzatore dispone di molteplici opzioni ed in particolare: il controllo a distanza del dispositivo infettato (l'operatore può servirsene senza limiti, compiendovi ogni tipo di attività); la visualizzazione di tutte le operazioni compiute dal detentore; la visualizzazione e l'estrazione di tutti i dati contenuti nel dispositivo; la sua messa fuori uso; l'attivazione del microfono e della webcam del dispositivo e quindi la possibilità di ottenere riprese audio e video.

In sostanza, **l'operatore ha il completo controllo non solo delle attività informatiche compiute dall'utilizzatore del dispositivo ma anche dei suoi movimenti e delle sue comunicazioni**. Quasi della sua vita, si potrebbe dire.

2) I discordanti indirizzi interpretativi sull'uso di virus informatici in funzione intercettiva

Sono poche ma piuttosto significative le decisioni di legittimità che si riferiscono al tema in esame.

Un primo caso fu risolto dalla quinta sezione penale della Corte di Cassazione con la **sentenza n. 16556 del 14 ottobre 2009**.

Un PM aveva disposto l'acquisizione in copia, ai sensi dell'articolo 234 del codice di procedura penale,

della documentazione informatica memorizzata all'interno del PC di un indagato. La novità stava nel fatto che l'acquisizione era stata ottenuta non, come solitamente avviene, con un decreto di sequestro ma mediante l'uso di un captatore informatico.

La difesa eccepì che, a dispetto del richiamo all'articolo 234, il PM aveva di fatto dato vita ad un'intercettazione che doveva essere considerata illegittima per difetto di autorizzazione.

La Corte di Cassazione rigettò il ricorso.

I giudici di legittimità osservarono anzitutto che "*per flusso di comunicazioni deve intendersi la trasmissione, il trasferimento, di presenza o a distanza, di informazioni da una fonte emittente ad un ricevente, da un soggetto ad altro, ossia il dialogo delle comunicazioni in corso all'interno di un sistema o tra più sistemi informatici o telematici*". Il PM si era invece limitato a disporre una semplice operazione di estrazione dati i quali avevano ad oggetto non flussi di comunicazioni ma "*una elaborazione del pensiero e la sua esternazione in scrittura su di un personal computer oppure mediante simboli grafici apposti su un supporto cartaceo, in un documento informatico realizzato mediante un sistema di videoscrittura ed in tal modo memorizzato*". Si era quindi mosso nell'ambito dell'articolo 189 codice di procedura penale dando vita cioè ad una prova atipica.

Negli anni successivi le cose si complicarono, come era facilmente prevedibile.

Una volta che una tecnologia è disponibile, è chiaro che la tendenza è di utilizzarla in ogni direzione possibile e questo vale in ogni ambito, ivi compreso quello giudiziario.

Le nuove frontiere applicative sono venute più volte all'attenzione della sesta sezione penale della Corte di Cassazione e, come si vedrà, la risposta è stata tutt'altro che univoca.

Viene anzitutto in rilievo, in ordine temporale, la **sentenza n. 24237 del 2015**.

Un tale era stato destinatario di un'ordinanza custodiale in carcere in quanto gravemente indiziato del delitto ex articolo 416 bis del codice penale. Il suo difensore aveva presentato istanza di riesame al competente Tribunale con esito negativo. Fece quindi ricorso per cassazione.

I più pregnanti motivi di impugnazione facevano rilevare che i gravi indizi a carico dell'indagato erano stati ottenuti con un'intercettazione realizzata tramite un virus informatico che aveva consentito la captazione del traffico dati dei smartphone bersaglio e delle conversazioni tra presenti avvenute nel raggio d'azione di tali apparecchiature delle quali erano stati attivati da remoto il microfono e la videocamera.

Il difensore del ricorrente aveva eccepito che l'intercettazione così disposta sfuggiva per sua natura a qualsiasi restrizione spaziale e temporale e consentiva un controllo indiscriminato dell'intera vita privata dei soggetti intercettati e di coloro che gli stavano vicini.

Era ben possibile, peraltro, che l'intercettazione, secondo gli spostamenti effettuati dal destinatario, avvenisse all'interno dei luoghi abitativi o di privata dimora senza che vi si stesse svolgendo alcuna attività criminosa.

Il collegio di legittimità ha rigettato il ricorso, limitandosi ad osservare che, vertendosi in un procedimento per delitti di criminalità organizzata, l'intercettazione tra presenti nei luoghi di privata dimora e affini non richiedeva il fondato motivo che vi si stesse svolgendo un'attività criminosa.

Ben diversa è stata la risposta che la stessa sezione ha dato alla medesima questione un paio di mesi più tardi con la **sentenza n. 27100/2015**.

L'iter logico seguito dai giudici di legittimità può essere così sintetizzato:

- l'attivazione da remoto del microfono dà certamente luogo ad **un'intercettazione ambientale** (rectius, **tra presenti**);
- l'articolo 266 comma 2 codice di procedura penale che regola questa tipologia intercettiva deve essere

interpretato nel senso che esso si riferisce alla captazione di conversazioni che avvengono in un determinato luogo e non dovunque; se così non fosse, risulterebbe violato l'articolo 15 della Costituzione che vieta di attribuire alle intercettazioni ambientali una latitudine così ampia da risultare indeterminata;

- la specifica tecnica intercettiva usata nel caso concreto è quindi inammissibile poiché consente la captazione in qualunque luogo si rechi l'utilizzatore dello smartphone controllato;
- l'unico modo per ricondurre a legittimità tale tecnica è allora che il **decreto autorizzativo** individui con precisione e preventivamente i luoghi nei quali è consentita la captazione;
- la logica conseguenza è che non sono utilizzabili le captazioni acquisite in luoghi diversi da quelli previamente specificati; se nessun luogo è stato indicato, nessuna captazione è utilizzabile;
- l'attivazione da remoto della videocamera dà invece vita da ad una prova atipica ex articolo 189 del codice di procedura penale ma non può essere espletata dovunque e senza limiti; è infatti vietata (ed i suoi risultati sono inutilizzabili) se riguarda ambiti domiciliari e deve invece essere autorizzata preventivamente con decreto motivato se è in grado di violare la riservatezza personale (come avverrebbe, ad esempio, se fosse inquadrato un bagno pubblico).

Sulla base di tali presupposti interpretativi, la sesta sezione ha accolto il ricorso ed annullato l'ordinanza impugnata.

3) La rimessione degli atti alle Sezioni unite

La querelle interpretativa è proseguita anche nell'anno in corso.

La sesta sezione penale è stata nuovamente chiamata in causa e, con la **decisione n. 13884/2016**, si è pronunciata nei termini che saranno immediatamente esposti.

La questione di partenza è identica ai casi precedenti sicchè se ne omette la ripetizione.

Il collegio ha anzitutto osservato che "*con riferimento alla tecnica dell'agente intrusore la pretesa di indicare con precisione e anticipatamente i luoghi interessati dall'attività captativa è incompatibile con questo tipo di intercettazione, che per ragioni tecniche prescinde dal riferimento al luogo, in quanto è collegata al dispositivo elettronico, sia esso smartphone o tablet ovvero computer portatile, sicché l'attività di captazione segue tutti gli spostamenti nello spazio dell'utilizzatore. Ovviamente questo comporta l'oggettiva impossibilità per il giudice di conoscere preventivamente gli spostamenti della persona che ha in uso il dispositivo elettronico sottoposto ad intercettazione e, quindi, di non poter dare indicazioni sui luoghi*".

I giudici si sono quindi chiesti se questa impossibilità e l'omessa indicazione dei luoghi che ne deriva determinino l'inutilizzabilità dei risultati dell'intercettazione.

Hanno al riguardo riconosciuto che **l'uso dell'agente intrusore dà luogo ad un'intercettazione tra presenti**.

Data questa premessa, gli è stato agevole rilevare che l'indicazione specifica del luogo assume importanza solo quando la captazione debba avvenire in abitazioni o altri luoghi privati. Non perché l'indicazione corrisponda di per se stessa a un obbligo normativo ma perché serve a delimitare i luoghi ai quali riferire la verifica dell'attualità dello svolgimento di un'attività criminosa.

Ed allora, tenendo conto del carattere itinerante della captazione svolta tramite un virus informatico e della sostanziale inesigibilità non solo dell'indicazione preventiva dei luoghi della captazione ma anche del rispetto di tale eventuale indicazione (dal momento che i luoghi dipendono esclusivamente dagli spostamenti dell'utilizzatore del dispositivo controllato), **l'unico modo per salvaguardare il precetto normativo ex articolo 266 comma 2 è quello di destinare successivamente all'inutilizzabilità, previo il loro stralcio dal compendio procedimentale, le captazioni avvenute in violazione di legge**.

Va tuttavia riconosciuto – si osserva – che **anche questo accorgimento non è esente da rischi se si considera che nel procedimento *de libertate* il giudice si pronuncia normalmente sulla base dei brogliacci predisposti dalla polizia giudiziaria nei quali non sempre è agevole distinguere il luogo in cui è avvenuta la comunicazione d'interesse**. È quindi essenziale in questa fase l'apporto della difesa.

Il problema in esame risulta comunque privo di impatto allorchè le intercettazioni siano disposte nell'ambito di un procedimento per fatti di criminalità organizzata poiché opera in questo caso l'articolo 13 del Decreto Legge 152/1991 che disancora la legittimità dell'operazione dal requisito dell'attività criminosa in corso.

Per tutte queste argomentazioni il collegio di legittimità ha ritenuto di non poter condividere la pronuncia contenuta nella sentenza n. 27100/2015.

Ha quindi ravvisato un contrasto interpretativo ed ha trasmesso gli atti alle Sezioni unite, formulando i seguenti tre quesiti:

- 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'articolo 266, comma 2, codice di procedura penale;
- 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.

4) Le argomentazioni del PG presso la Corte di Cassazione

A brevissima distanza di tempo, precisamente il 28 aprile 2016, le Sezioni unite si sono pronunciate sulla questione.

Si ritiene utile tuttavia, prima di dar conto della soluzione prescelta, riportare i passaggi salienti della **memoria depositata per l'occasione dalla Procura generale presso la Corte di Cassazione**.

Si tratta di un documento di indubbio interesse sia per l'autorevolezza della fonte che per la qualità delle argomentazioni sicchè viene naturale inserirlo tra i contenuti che meglio consentono di comprendere la questione in esame.

La prima considerazione del PG è apertamente metagiuridica.

Egli constata la straordinaria velocità dei progressi delle tecnologie della captazione e, in parallelo, di quelle volte all'elusione della captazione (fondate in massima parte sulle tecniche di criptazione).

Ne trae la convinzione che **l'impiego di virus informatici, più che al potenziamento delle intercettazioni, serve in realtà a recuperare l'efficacia perduta o compromessa delle tecniche tradizionali**.

Invita quindi le Sezioni unite ad inserire anche questa esigenza nel complesso *balance* degli interessi e dei valori in gioco.

La memoria del PG passa quindi a descrivere le caratteristiche tecniche del Trojan horse e giunge ad una

particolare conclusione. Vero che questo mezzo consente una molteplicità di funzioni ma ugualmente vero che proprio questa molteplicità consente l'apposizione di limiti tecnici preventivi al suo utilizzo. La legge e il diritto hanno quindi la possibilità di regolamentarne l'uso nella direzione che gli pare più opportuna alla luce dei precetti costituzionali.

Il passaggio successivo riguarda la legittimità dell'uso di questo strumento nei procedimenti per delitti di criminalità organizzata.

Il PG si concede uno spazio definitorio e nega ogni legittimazione alla locuzione "*intercettazioni ambientali* ".

Per un questione di lessico normativo, anzitutto, non avendo mai il legislatore impiegato questa espressione, ma soprattutto perché gli preme sgomberare il campo da tutte le enfatizzazioni del concetto di ambiente connesse a quella locuzione.

In altre parole: è sbagliato in partenza qualunque ragionamento che, assumendo gli ambienti determinati come parametri ineludibili di riferimento, neghi legittimazione ad intercettazioni tra presenti che prescindano dai parametri medesimi.

La conclusione è a questo punto conseguenziale: **sbaglia la sentenza n. 27100/2015 quando, anziché rifarsi all'unica distinzione normativamente consentita** – quella tra intercettazioni tra presenti e intercettazioni tra presenti in luoghi di abitazione o privata dimora – **assume come riferimento la distinzione, priva di riscontro normativo, tra intercettazioni in ambienti predeterminati e intercettazioni prive di tale predeterminazione**.

Il secondo errore di quella decisione è di non avere attribuito alcun rilievo all'articolo 13 del Decreto Legge 152/1991 e di avere quindi omesso di considerare la sua portata derogatoria rispetto alla previsione ordinaria contenuta nell'articolo 266 comma 2 codice di procedura penale.

Queste pecche motivazionali hanno fatto sì che la sentenza citata si discostasse dalla consolidata giurisprudenza precedente che aveva richiesto l'indicazione specifica dei luoghi dell'attività intercettiva solo per le intercettazioni disposte in procedimenti ordinari.

Chiarito questo punto, il PG passa ad esaminare i peculiari problemi posti dall'uso del captatore informatico nelle intercettazioni tra presenti.

Ritiene comunque necessario ricordare che nel procedimento de quo il GIP aveva espressamente negato l'autorizzazione all'uso del captatore per l'effettuazione di videoriprese e non risulta peraltro che siano stati acquisiti i contenuti dell'apparecchio controllato.

Stando così le cose, e non venendo quindi in rilievo modalità intercettive diverse dalla semplice captazione di conversazioni tra presenti, **il PG è dell'avviso che le norme vigenti consentano senz'altro e senza alcuna eccezione le intercettazioni foniche a mezzo virus informatico nei procedimenti che si occupano di criminalità organizzata**.

Il presupposto logico è che il legislatore, attraverso la normativa del 1991, ha effettuato un adeguato bilanciamento degli interessi in campo e, per così dire, ha accettato il prezzo di consentire intercettazioni in luoghi di privata dimora o abitazione anche se non vi si stia svolgendo alcuna attività penalmente rilevante.

Il PG ha di seguito escluso che lo strumento di indagine di cui si parla confligga in qualche modo con precetti costituzionali.

Di certo, non con l'articolo 15 della Costituzione che è soddisfatto con l'emissione di un atto motivato dell'autorità giudiziaria che sia rispondente alla normativa vigente.

Ma neanche con l'articolo 14 della Costituzione alla luce dei chiarissimi principi affermati dalla Consulta nella sentenza n. 135/2002 che ha escluso l'esistenza di un divieto costituzionale assoluto alla captazione di

immagini in luoghi di privata dimora e demandato al giudice il compito di stabilire quali riprese siano finalizzate alla captazione di comportamenti di tipo comunicativo.

Del pari, secondo il PG, nessuna violazione dell'articolo 8 CEDU può razionalmente derivare dall'uso dei virus informatici come mezzi di intercettazione.

Dopo un dettagliato excursus giurisprudenziale, viene richiamata in particolare la **sentenza emessa il 4 dicembre 2015 dalla Corte EDU nel caso Zakharov c. Russia** che contiene una sorta di decalogo dei requisiti necessari a rendere conformi all'articolo 8 le intercettazioni.

A giudizio del PG, la sentenza in esame menziona sì il requisito dell'indicazione dei luoghi ma lo considera come alternativo all'identificazione della persona da sorvegliare.

Tutti gli altri requisiti sono perfettamente rispettati dalla normativa italiana, anche se interpretata nel senso di consentire la tecnica intercettiva del virus informatico.

In particolare, la crescente pericolosità delle organizzazioni terroristiche fa sì che sia certamente ravvisabile la necessità della misura in una società democratica.

Il PG si è infine soffermato sull'identificazione della categoria dei delitti di criminalità organizzata indicata nel più volte citato articolo 13. Ha ravvisato la necessità che le Sezioni unite ne definiscano con chiarezza il contenuto, proponendo l'uso dell'elenco contenuto nell'articolo 407 comma 2 lettera a) codice di procedura penale.

Date queste premesse, il PG ha concluso chiedendo che le Sezioni unite affermino:

- **l'ammissibilità dell'intercettazione tramite virus informatico nei procedimenti per delitti di criminalità organizzata senza necessità di predeterminazione dei luoghi** (terzo quesito);
- **le intercettazioni svolte in luoghi di abitazione o privata dimora nell'ambito di procedimenti ordinari richiedono invece la predeterminazione degli ambienti da controllare** in quanto indispensabile prerequisito per la verifica dell'attualità dello svolgimento di un'attività criminosa (primo quesito);
- **le captazioni acquisite in luoghi privati al di fuori dei presupposti di cui all'articolo 266 comma 2 codice di procedura penale non sono inutilizzabili** poiché tale sanzione è riservata a gravi patologie degli atti procedimentali mentre nel caso di specie si tratterebbe di rimediare ad una situazione dovuta agli effetti imprevedibili e incontrollabili del decreto autorizzativo (secondo quesito);
- sarebbe quindi preferibile negare in radice ogni legittimità all'uso dei virus informatici in procedimenti ordinari.

Questa è in sintesi la visione del nostro massimo organo giudiziario requirente.

5) L'intervento chiarificatore delle Sezioni unite

Dal canto loro le Sezioni unite hanno risolto la questione, chiarendo che **anche nei luoghi di privata dimora ex articolo 614 del codice penale, pure non singolarmente individuati e anche se ivi non si stia svolgendo l'attività criminosa, è consentita l'intercettazione di conversazioni o comunicazioni tra presenti, mediante l'installazione di un captatore informatico in dispositivi elettronici portatili.**

L'intercettazione è tuttavia limitata ai procedimenti per delitti di criminalità organizzata, anche di tipo terroristico, per tali dovendosi intendere quelli elencati nell'articolo 51 commi 3 bis e 3 quater codice di procedura penale nonché gli altri "*comunque facenti capo ad un'associazione per delinquere, con esclusione del mero concorso di persone nel reato*".

La soluzione appena riportata è allo stato ricavata esclusivamente dall'informazione provvisoria diramata dalla Corte suprema, non essendo ancora disponibile la motivazione.

6) Riflessioni sulla decisione delle Sezioni unite

Gli interventi delle Sezioni unite condividono in genere tre caratteristiche essenziali.
La prima è strettamente connaturale alla funzione nomofilattica dell'organo: le sue pronunce indicano una soluzione interpretativa che, se credibile e convincente, si tramuta in diritto vivente, dirada confusione e conflitti, favorisce la prevedibilità e la condivisione delle scelte giurisdizionali.
La seconda si traduce in una sorta di warning al legislatore: le Sezioni unite intervengono quando ci sono conflitti interpretativi e questi sono generalmente dovuti a norme di significato incerto o di contenuto discutibile oppure inadeguate alle esigenze contemporanee oppure a discipline carenti o addirittura omissive.
La terza ragione è meno appariscente ma non per questo di minore importanza. Il fatto stesso che le Sezioni unite prendano in carico una questione giuridica equivale ad accendere una **spia luminosa**: la nostra massima istanza giurisdizionale avverte che si tratta di qualcosa a cui tutti, non solo i membri della comunità giuridica, devono prestare attenzione perché è destinato ad avere riflessi non solo sui processi ma anche sulle vite dei consociati, sul modo in cui i loro diritti e doveri si compongono in un equilibrio più generale, sul livello di garanzie che l'ordinamento è disposto a riconoscere e così via.
Pare innegabile, pur con la cautela imposta dalla disponibilità di una semplice informazione provvisoria, che il pronunciamento delle Sezioni unite qui commentato presenti tutte queste caratteristiche.
Ciò detto, la soluzione prescelta – questo è già chiaro – **dà il via libera all'uso dei virus informatici allorchè si intenda ricorrere ad intercettazioni in procedimenti per delitti di criminalità organizzata**.
Questa modalità diventerà quindi – e anche questa è una facile previsione – di uso comune e massivo nelle attività investigative delle DDA.
Viene per ciò stesso colmato o almeno attenuato il gap tecnologico cui il PG ha destinato la prima considerazione della sua memoria. Se ne creeranno altri, è ovvio, ma per intanto gli organi inquirenti sono messi in condizione di usare le più avanzate tecnologie captative disponibili e il Trojan horse aggiunge legittimamente alle sue varie possibili denominazioni (programma informatico, malware, agente intrusore, captatore informatico, spyware) quella di virus di Stato.
Come sempre, l'interrogativo primario è comprendere quali saranno gli effetti, giuridici e non, che questa nuova possibilità produrrà nello scenario del nostro Paese.

6.1) Gli effetti giuridici connessi all'eventuale violazione dell'articolo 266 comma 2 codice di procedura penale.

Le Sezioni unite hanno compiuto l'attività definitoria esplicitamente richiesta dal PG, chiarendo che la qualifica di procedimenti per delitti di criminalità organizzata spetta a quelli rientranti nella previsione dei commi 3° bis e quater dell'articolo 51 codice di procedura penale e agli altri in cui si procede per reati comunque facenti capo ad un'associazione a delinquere.
La formulazione dell'ultimo inciso, pur non chiarissima, sembra comunque autorizzare l'estensione di quella qualifica a qualsiasi procedimento in cui si contesti un qualunque delitto purchè ascrivibile al programma criminoso di un'associazione a delinquere.
Spetta ovviamente al PM, per fisiologia ordinamentale, individuare e circostanziare le fattispecie di reato che ritiene più congrue al fatto sottostante.
Sicchè è una parte, sia pure pubblica ed al servizio di fini pubblici, a determinare le condizioni che consentono la particolare metodica intercettiva di cui si parla.
Basta quindi, ad esempio, che un PM iscriva nel registro delle notizie di reato un delitto ordinario aggravato ex articolo 7 Decreto Legge 152/1991 oppure compreso nel programma criminoso di un'associazione a delinquere ed ha per ciò stesso, in base al criterio fissato dalle Sezioni unite, posto le

condizioni per l'uso del Trojan horse.
Occorre allora chiedersi cosa potrebbe accadere se, a posteriori, si accerti che la qualificazione delle fattispecie operata inizialmente sia erronea.
In altre parole: **che sorte avrebbero le captazioni acquisite sulla base di un decreto autorizzativo che non indica luoghi specifici e non consente quindi di verificare il fondato motivo di ritenere l'attualità di una condotta criminosa in un certo luogo**, se poi fosse giudizialmente accertato che il delitto di criminalità organizzata inizialmente ipotizzato non esisteva o che il delitto comune che si assumeva in un programma associativo non aveva invece questa caratterizzazione?
Già la sola rassegna giurisprudenziale contenuta nei paragrafi precedenti dimostra l'inesistenza di risposte univoche.
Si ricorderà che, secondo la sentenza 27100/2015, le intercettazioni tra presenti sono legittime solo se precedute da un decreto autorizzativo che individui in modo chiaro e preciso i luoghi nei quali è consentita la captazione. Sono quindi inutilizzabili, secondo questa visione, sia le captazioni acquisite in luoghi diversi da quelli predeterminati sia, a maggior ragione, quelle acquisite in assenza di qualsiasi indicazione.
Si ricorderà ugualmente che la decisione 13884/2016 ha espresso una visione assai differente.
Ha considerato infatti inesigibile in fatto, a fronte dell'uso di un agente intrusore di tipo informatico, la pretesa di un'indicazione preventiva dei luoghi interessati dall'attività captativa.
Ha però ammesso l'esistenza del rischio, collegato all'inesistenza di filtri preventivi, che siano acquisite captazioni ottenute nei luoghi ex articolo 614 del codice penale.
Ha quindi manifestato l'opinione che le medesime, nei casi in cui siano state ottenute in violazione di legge - possibilità evidentemente limitata ai procedimenti in cui non si procede per delitti di criminalità organizzata - debbano essere sanzionate con l'inutilizzabilità da dichiararsi dopo il completamento delle operazioni di intercettazione.
Va peraltro sottolineato che, proprio a questo proposito, il collegio della sesta sezione ha ritenuto di porre uno specifico quesito alle Sezioni unite, volto a chiarire se la sanzione di inutilizzabilità dovesse limitarsi alle captazioni avvenute in luoghi di privata dimora in violazione dell'articolo 266 comma 2 del codice di procedura penale.
Il provvedimento di rimessione non ha esplicitato l'alternativa ma è logico immaginare che essa dovesse consistere nell'estensione dell'inutilizzabilità a tutte le captazioni, anche se acquisite in luoghi non di privata dimora.
Sempre a questo proposito, resta da dire che il relativo parere espresso dal PG è stato nel senso di non ravvisare alcuna inutilizzabilità nella situazione ipotizzata dal giudice rimettente. Ma questa valutazione presupporrebbe logicamente che il collegio della sesta sezione si fosse pronunciato in termini dubitativi sull'individuazione dell'inutilizzabilità come sanzione adeguata, il che non è avvenuto poiché l'unico dubbio era, come si è appena visto, sulla latitudine della sanzione.
La considerazione appena esposta permette di passare immediatamente alla terza soluzione proposta, cioè appunto quella del PG.
A suo giudizio – lo si ripete – le captazioni acquisite in luoghi privati al di fuori dei presupposti di cui all'articolo 266 comma 2 del codice di procedura penale non sono inutilizzabili poiché tale sanzione dovrebbe essere riservata a gravi patologie degli atti procedimentali mentre nel caso di specie si tratterebbe di rimediare ad una situazione dovuta agli effetti imprevedibili e incontrollabili del decreto autorizzativo.

L’unico rimedio possibile è allora quello di sbarrare totalmente la strada all’uso a fini intercettivi dei virus informatici nei procedimenti ordinari.

È infine a tutt’oggi ignoto il pensiero delle Sezioni unite per quest’aspetto poiché l’informazione provvisoria non contiene alcun’indicazione utile.

Sicchè, a ragionare esclusivamente sulla base degli indirizzi emersi finora nel circuito di legittimità, sarebbero possibili due opzioni: **la prima è l’inutilizzabilità, la seconda è una sorta di self restraint dei PM che dovrebbero sempre rinunciare ad avvalersi degli agenti intrusori informatici quando intendono dar vita ad intercettazioni nei procedimenti ordinari**.

Se questa è la cornice entro cui muoversi, bisogna adesso chiedersi cosa succederebbe con ciascuna delle due opzioni.

Quanto all’inutilizzabilità, è fin troppo noto il granitico indirizzo giurisprudenziale, originato da una pronuncia delle Sezioni unite, che nega l’esistenza di qualunque forma di inutilizzabilità derivata.

Ed allora, una volta affermata l’inutilizzabilità di una certa captazione, la sanzione non precluderebbe l’uso del suo risultato come *notitia criminis* e quindi, ad esempio, come legittimo input per la richiesta di una nuova sequenza intercettiva o per altre attività investigative.

Il frutto dell’albero avvelenato non sarebbe perciò considerato avvelenato anch’esso e non sarebbe condannato alla distruzione ma rimarrebbe a disposizione degli inquirenti per gli scopi predetti.

La seconda opzione viene proposta dal suo ideatore come unica soluzione possibile ma – non sembra azzardato dirlo – non risolve alcunchè. La sua concreta efficacia è infatti strettamente connessa alla discrezionalità del PM il quale, in assenza di divieti normativi o di eventuali linee guida cogenti all’interno dell’ufficio giudiziario in cui opera, potrebbe non tenerla affatto in considerazione e comportarsi quindi in tutt’altro modo.

Ma c’è di più. La stessa opzione non offre alcuna indicazione circa l’uso che debba farsi di captazioni ottenute in violazione del disposto dell’articolo 266 comma 2.

Si perdonerà l’ovvietà ma **ciò che non è inutilizzabile e non è altrimenti invalido rimane per ciò stesso in vita**.

Sicchè – ci si chiede – che uso dovrebbero fare le parti e il giudice di elementi conoscitivi che continuano a far parte del materiale procedimentale o del fascicolo dibattimentale? Possono legittimamente ignorarlo e non farne alcun uso? Oppure sono tenuti a confrontarsi con quegli elementi e dargli un significato, quale che sia?

Domande legittime alle quali manca allo stato qualsiasi risposta. Facile prevedere che si crei, almeno per questo specifico aspetto, la **confusione che pure l’intervento delle Sezioni unite avrebbe dovuto scongiurare**.

6.2) Controllabilità dell’uso del virus informatico

Così si legge testualmente nella più volte citata memoria del PG: *“La molteplicità di funzioni dei programmi informatici di cui si discute non deve indurre a credere di essere di fronte a strumenti onnipervasivi e onnipotenti, suscettibili di dar vita ad un potere invasivo esercitabile senza limiti o in forme incontrollabili sotto il profilo tecnico o giuridico.*

Al contrario è seriamente ipotizzabile l’apposizione di limiti tecnici preventivi all’impiego dei virus informatici (ad es., inibendo a priori l’operatività di alcune delle loro molteplici funzioni acquisitive).

Inoltre, ciò che più conta in questa sede, è possibile dettare i limiti giuridici delle modalità di utilizzo dei captatori (ad es. escludendo che i programmi di on line surveillance possano essere utilizzati per effettuare videoriprese o che i programmi on line search siano impiegati per acquisire dati, al di fuori o in contrasto con le regole in tema di perquisizioni e sequestri).

Ancora una volta , dunque, come avviene del resto in altri delicatissimi campi dell'esperienza umana, sono la legge ed il diritto a fissare i confini delle possibilità offerte dalla tecnologia, commisurandole ai principi dello Stato democratico di diritto, ai diritti individuali ed alle esigenze e sensibilità della collettività".

L'opinione è chiara: non bisogna avere paura delle conquiste tecnologiche e delle loro applicazioni pratiche, perché è senz'altro possibile apporre limiti tecnici al loro uso (nel caso di specie selezionando le funzioni acquisitive indispensabili ed escludendo tutte le altre) e perché si possono porre altrettanti limiti giuridici.

Il ragionamento è rassicurante ma la situazione è davvero quella descritta dal PG?

Per farsi un'idea più precisa, può servire la storia di una società italiana, di cui si omettono i riferimenti perché non essenziali, che opera nel settore dell'information technology e che risulta l'unica produttrice del programma Trojan horse.

Il suo core business è ben descritto da Carola Frediani[1].

Questa società ha conquistato più volte l'attenzione degli organi di stampa[2].

Ed allora, volendo riassumere: un'azienda alla quale le istituzioni pubbliche italiane si rivolgono frequentemente quando intendono acquistare spyware del tipo Trojan è stata hackerata, perdendo dati di interesse strategico che potrebbero essere finiti in mani sbagliatissime; sempre quell'azienda vende prodotti della stessa specie a Stati ed agenzie i cui interessi potrebbero essere in conflitto con quello nazionale.

In Italia, peraltro, operano almeno **sette società specializzate non solo nelle intercettazioni telefoniche ma anche nel monitoraggio del traffico Internet, dei servizi di messaggistica istantanea o via sms e di tracciamento via GPS e in ulteriori e più sofisticati servizi.**

Una di esse, che ha tra l'altro collaborato professionalmente con un'importante Procura italiana, fu implicata nella rivelazione indebita di una conversazione intercettata tra un autorevole esponente politico e un alto dirigente bancario a proposito della scalata ad un primario istituto di credito[3].

Altre sono specializzate nella ***virtual humint***, cioè la creazione a fini investigativi di finti profili sui social media. Si tratta di **fittizie identità on line** che possono essere tenute in vita per anni e che consentono di infiltrarsi in gruppi e comunità che si desidera tenere sotto osservazione.

Altre ancora operano direttamente nel **campo dell'intelligence vera e propria**, cioè sono in grado di analizzare e classificare grandi quantità di dati e documenti, traendoli dal web, da forum, blog e quant'altro, e trarne conclusioni su tendenze e specifiche attività.

Altre, infine, operano in particolare nel **settore delle apparecchiature di sorveglianza sotto copertura e tracciamento.**

Prendendo a prestito le parole di Luca Rinaldi, si tratta di "*un comparto che negli ultimi anni … è cresciuto a dismisura, alimentando un esercito di controllori senza controlli. Di sicuro … il Belpaese, almeno nel settore privato, rimane uno dei più attivi a livello mondiale nello sviluppo di tecnologie e software per il monitoraggio e tracciamento di comunicazioni e spostamenti*".

Che le cose non siano proprio rassicuranti e che non tutti condividano il senso di sicurezza manifestato dal PG, lo si ricava anche dall'iter travagliato di alcune proposte di legge in materia e dal convulso dibattito politico che le ha accompagnate.

Si pensi, ad esempio, al cosiddetto **decreto antiterrorismo**, vale a dire il Decreto Legge 7/2015 convertito

nella Legge 43/2015. Nella stesura iniziale del testo era stata inserita un'aggiunta all'art. 266 bis c.p.p. tale per cui l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra più sistemi sarebbe stata consentita "*anche attraverso l'impiego di strumenti o di programmi informatici per l'acquisizione da remoto delle comunicazioni e dei dati presenti in un sistema informatico*".

La proposta non è sfuggita all'attenzione di commentatori qualificati.

Così ne ha parlato, tra gli altri, Stefano Quintarelli, deputato, informatico di professione e attuale presidente del Comitato di indirizzo dell'Agenzia per l'Italia digitale: "*L'uso di captatori informatici (trojan, keylogger, sniffer,...) quale mezzo di ricerca delle prove da parte delle Autorità Statali (giudiziarie o di sicurezza) è controverso in tutti i paesi democratici per una ragione tecnica: con quei sistemi viene compiuta una delle operazioni più invasive che lo Stato possa fare nei confronti dei cittadini, poiché quella metodologia è contestualmente una ispezione, una perquisizione, una intercettazione di comunicazioni, una acquisizione occulta di documenti e dati anche personali; tutte attività compiute in un luogo, i sistemi informatici privati, che equivalgono al domicilio. E tutte quelle attività vengono fatte al di fuori delle regole e dei limiti dettate per ognuna di esse dal Codice di Procedura Penale*"[4].

Preoccupazioni di ugual genere sono state espresse da **Antonello Soro, attuale presidente dell'Autorità garante per la protezione dei dati personali**, secondo il quale "*perplessità suscita anche l'emendamento che ammette le intercettazioni preventive (disposte dall'autorità di pubblica sicurezza nei confronti di meri sospettati), per i reati genericamente commessi on-line o comunque con strumenti informatici. Anche in tal caso l'equilibrio tra protezione dati ed esigenze investigative sembra sbilanciato verso queste ultime*".

Il risultato di opinioni come queste è stato lo stralcio della modifica dell'articolo 266 bis che è quindi scomparsa dal testo definitivo.

E tuttavia la questione non si è chiusa lì.

Difatti, il 2 dicembre 2015 la deputata Maria Gaetana Greco ha presentato alla Camera una proposta di legge la cui relazione inizia così: "*I recenti episodi verificatisi in Europa, e più in generale nel mondo, hanno evidenziato l'innalzamento della minaccia terroristica che, presentandosi in forme spesso nuove e di inusitata violenza, costituisce una gravissima insidia per la sicurezza interna e internazionale, nonché un fattore di instabilità dell'intero quadro geo-politico. Tale contesto ha reso ormai improrogabile lo sviluppo di una capacità di risposta globale attraverso misure da adottare sia sul versante interno che su quello internazionale, anche per offrire una risposta strategicamente efficace […] Tra queste misure va senz'altro considerata la possibilità di consentire alle Forze di polizia l'utilizzo di nuovi programmi informatici che permettano l'accesso da remoto ai dati presenti in un sistema informatico al fine di contrastare preventivamente i reati di terrorismo commessi mediante l'uso di tecnologie informatiche o telematiche*".

Si ripropone in sostanza, a stretto ridosso del sanguinario attentato al Bataclan di Parigi e nel clima emotivo di quei giorni, l'uso del Trojan di Stato.

È degno di nota che la proposta sia sostanzialmente identica a quella che avrebbe dovuto essere contenuta nel decreto antiterrorismo.

Così ne parla l'avvocato e giornalista Guido Scorza[5]: "*Ora, però, l'On. Greco sembra intenzionata a riprovarci e lo fa utilizzando le stesse identiche parole, una per una, attraverso le quali, all'epoca – era il febbraio del 2015 – si sarebbe già voluto far posto al trojan di Stato tra gli strumenti di indagine a disposizione di investigatori e forze dell'ordine.*

Neppure una parola in più, neppure un principio, un paletto o un vincolo in più per scongiurare il rischio che la sacrosanta esigenza di dotare chi difende la sicurezza pubblica di efficaci strumenti di indagine scivoli in una violazione massiccia della privacy dei cittadini come, purtroppo, sta accadendo in mezza

Europa proprio sulla scia dei drammatici fatti di Parigi che appaiono legati ad un rapporto di causa-effetto anche all'iniziativa dell'on. Greco".

Merita infine di essere citata, per la sua incisività, l'opinione espressa qualche anno addietro, quando ancora l'uso del Trojan a fini intercettivi era di là da venire, da Carlotta Conti: "*è indispensabile sottolineare come, al giorno d'oggi, all'interno della categoria delle prove atipiche ricadano molte insidiose violazioni della riservatezza e/o di altri diritti fondamentali. Si pensi alla questione dei numerosi virus informatici idonei a captare tutti i dati che vengono inseriti all'interno di un personal computer. Sul punto, la Cassazione è intervenuta nel 2010 escludendo la lesione di diritti fondamentali ed annoverando l'atto tra i mezzi atipici di ricerca della prova. Eppure siffatte attività pervengono ad un livello di aggressione della riservatezza individuale che sfiora l'inviolabilità della psiche e, forse, la questione meriterebbe una maggiore attenzione*"[6].

Si potrebbe continuare ma c'è già quanto basta a farsi un'idea.

Non pare possa mettersi in dubbio che le intercettazioni in generale, e l'uso di spyware in particolare, pongano complessi problemi che hanno a che fare con l'affidabilità dell'operatore privato chiamato a compiere e gestire le operazioni tecniche necessarie e l'affidabilità della tecnologia di cui l'operatore fa uso.

Il primo punto è se, come sostiene il PG, siamo in grado di prevenire senza difficoltà quei rischi e comunque di eliminarne gli effetti negativi oppure no.

Il secondo è se l'uso di tecnologie così sofisticate, rischiose e invasive possa essere consentito da un indirizzo interpretativo, per quanto autorevole ne sia la fonte, oppure sia doveroso attendere l'intervento del legislatore.

Ancora domande, come si vede, ma il fatto stesso che sia possibile porle rende in qualche modo più precaria l'architettura della costruzione giurisprudenziale in esame.

6.3) Cosa ne pensa la Corte di Strasburgo

Come si è evidenziato in precedenza, il PG, perfettamente consapevole del rilievo che in materia deve essere riconosciuto alla previsione dell'articolo 8 CEDU, ha inteso confrontarsi con la giurisprudenza della Corte EDU di Strasburgo, unica istanza legittimata ad interpretare le norme convenzionali.

La conclusione del PG è stata di assoluta conformità alla lettera ed allo spirito dell'articolo 8 dell'interpretazione proposta alle Sezioni unite.

Il perno principale su cui si è fondata la valutazione del PG è la sentenza che la Corte EDU ha emesso il 4 dicembre 2015 nel caso Zakharov c. Russia.

È stato valorizzato in particolare il passaggio, contenuto nei punti 264 e 265 della motivazione, in cui si afferma (il testo ufficiale è in lingua inglese ma qui si usa una traduzione non ufficiale in italiano) che "*per quanto riguarda il contenuto dell'autorizzazione all'intercettazione, esso deve chiaramente identificare una persona specifica da porre sotto sorveglianza o un singolo insieme di luoghi corrispondente a quelli per i quali l'autorizzazione è stata concessa. Tale identificazione può essere fatta per mezzo di nomi, indirizzi, numeri di telefono o altre informazioni rilevanti"*.

Il PG ha in sostanza sottolineato che ciò che rende legittima un'attività intercettiva è l'indicazione della persona che la subisce o, in alternativa, dei luoghi in cui sarà svolta. Il che dimostra che la predeterminazione localistica non è di per se stessa indispensabile ove si possa contare sull'identificazione del destinatario.

Vero.

Bisogna però ricordare che la Corte di Strasburgo richiede ormai da tempo il requisito della **qualità della legge in materia di intercettazioni**

e, tra le condizioni necessarie perché possa parlarsi di qualità accettabile, vi è quella che consente al cittadino di comprendere esattamente quali siano l'ampiezza e i limiti del potere discrezionale dell'autorità nazionale che ha il potere di ingerenza nella sfera protetta.

Sarebbe piuttosto arduo sostenere che la vigente regolamentazione normativa italiana in materia di intercettazioni consenta ai consociati di avere ben chiaro che, andandosene a spasso con i loro smartphone o incrociando qualcun altro che fa lo stesso oppure semplicemente entrando nel raggio d'azione del microfono o della videocamera del suo dispositivo, corrano per ciò stesso il rischio che i loro movimenti, le loro parole, i loro gesti siano suscettibili di essere immortalati per esigenze giudiziarie.

Non basta: **la CEDU e la Corte che ne è custode richiedono che l'ingerenza sia necessaria in una società democratica**. Si tratta di un requisito che, forse volutamente, è vago e generico. La sua più comune interpretazione è comunque connessa all'esigenza di un equilibrio e quindi di un'adeguata proporzionalità tra la portata dell'ingerenza nella vita privata e il fine perseguito da chi esercita quell'ingerenza. Per questa via, potrebbe essere ritenuta sproporzionata anche una legittima intercettazione se le ripercussioni da essa create nella vita del singolo appaiano sovradimensionate rispetto all'interesse collettivo.

Vale infine la pena ricordare, a chiusura ed en passant, che nel **caso Lambert c. Francia (sentenza Corte EDU del 24 agosto 1998)** fu fissato il principio secondo il quale il quale la legge deve stabilire delle garanzie sufficienti non solo per il titolare della linea telefonica intercettata ma anche per il terzo che, chiamando o chiamato da tale linea, riceva delle conseguenze dall'intercettazione della sua conversazione.

Viene da immaginare, in conclusione, che la Corte di Strasburgo, se si trovasse investita di un ricorso che in qualche modo ponesse alla sua attenzione captazioni ottenute tramite la rete a strascico degli spyware, avrebbe forse qualcosa di più da dire rispetto all'opinione del PG.

Conclusione

La questione su cui si è riflettuto è estremamente attuale il che, se concorre a renderla interessante, impedisce però di contare su opinioni consolidate e, ciò che più conta, su verifiche sul campo che chiariscano se le preoccupazioni manifestate siano fondate o piuttosto il frutto di un timore irrazionale verso il "nuovo che avanza".

Si vedrà.

Certo è che gli Stati si trovano ad affrontare minacce criminali ogni giorno più complesse e insidiose e a doversi confrontare con scenari caratterizzati da contrapposizioni ideologiche, etniche, religiose, culturali che costituiscono il terreno ideale per temibili sfide alla pace e alla sicurezza sociale.

In tutto questo le nuove conquiste scientifiche e tecniche mettono a disposizione di chiunque possibilità, lecite e illecite, altrettanto complesse e versatili e inducono quindi una domanda incessante di tecnologia e innovazione.

La cosa è in sé neutra, né giusta né sbagliata, e non può comunque essere fermata, essendo illusorio ogni tentativo di rallentare i progressi umani o di indirizzarli verso percorsi predeterminati.

Si può e si deve invece fare quanto possibile perché i nuovi saperi e le nuove tecnologie vengano usati in modo da non compromettere o sciupare i valori essenziali che tengono insieme la nostra civiltà e le danno senso.

Si può e si deve cercare il miglior equilibrio possibile tra difesa sociale e libertà dei consociati.

Sperando non tanto di indovinare tutte le scelte ma di sbagliarne il meno possibile.

[1] **C. Frediani**, articolo pubblicato il 16 settembre 2013 sull'edizione web della rivista Wired. Vi si legge che: "*Le* (sue) *origini … risalgono al 2001, quando due programmatori … scrissero* ***E.****, un software che faceva da "suite completa per attacchi man-in-the-middle", cioè un insieme di strumenti per sniffare password e dati, registrare conversazioni e chat, e controllare da remoto un computer target. La loro*

creazione piacque molto alla Questura di … che era interessata a usarlo nelle indagini. Da lì iniziò la carriera dell'azienda come venditore di Trojan a forze dell'ordine e agenzie statali di vari Paesi, cioè di malware in grado di infettare silenziosamente un computer, e da quel momento in avanti di averne pieno controllo e poterne monitorare tutta l'attività".

[2] Nell'edizione del 3 novembre 2015 di Repubblica.it Tecnologia si è data notizia di una perquisizione disposta da una Procura nei confronti di un'azienda sulla base del sospetto che i suoi gestori, in passato dipendenti della società prima menzionata, potessero essere coinvolti in un'azione di hackeraggio a danno di quest'ultima con la violazione di 400 gigabyte di dati riservati. L'ipotesi è che gli indagati si fossero impadroniti del codice sorgente dello spyware G., cioè il programma che la società fornisce a governi e forze dell'ordine, e lo abbiano poi ceduto ad una società saudita che potrebbe a sua volta averlo trasmesso a gruppi jihadisti.

Ancora più di recente la medesima società è stata nuovamente menzionata in un articolo di cronaca, curato anch'esso da Carola Frediani ma questa volta per l'edizione web di La Stampa Tecnologia del 7 aprile 2016.

La notizia è che il 31 marzo 2016 il Ministero dello sviluppo economico ha revocato l'autorizzazione all'export di cui godeva la società in direzione dei Paesi extra UE. Secondo l'articolista, la ragione del provvedimento sarebbe in qualche modo collegata al caso di Giulio Regeni ed al fatto che l'Egitto sarebbe tra i clienti della società medesima, assieme a numerosi altri Stati africani ed asiatici.

Vengono citate due interrogazioni parlamentari nelle quali si assume che essa avrebbe venduto i suoi spyware all'intelligence egiziana.

[3] **Luca Rinaldi**, articolo pubblicato sull'edizione web di Wired.it del 16 luglio 2015.

[4] La dichiarazione è riportata da **Michele Nasi** in un articolo pubblicato sull'edizione de IlSoftware.it del 27 marzo 2015.

[5] **G. Scorza**, articolo apparso sull'edizione web de Il Fatto quotidiano del 26 gennaio 2016.

[6] **C. Conti**: *Annullamento per violazione di legge in tema di ammissione, acquisizione e valutazione delle prove: le variabili giurisprudenziali* (relazione tenuta ad un incontro di formazione svoltosi il 13 dicembre 2012 presso la Corte di Cassazione)".

TAG: *criminalità organizzata, intercettazioni, privacy, Virus informatico, Criminologia, costituzionale, Diritto della privacy, Diritto delle nuove tecnologie e delle comunicazioni, penale, New technology, Procedura penale*
