Uno sguardo comparatistico sul bilanciamento tra libertà delle comunicazioni ed esigenze della sicurezza nazionale ed internazionale
Relazione al seminario della Scuola Superiore della Magistratura – Scandicci 11 maggio 2016

Giovanni Salvi

Premessa. La sicurezza nazionale e internazionale pone in questione l'utilizzo di strumenti di prevenzione e di contrasto in parte diversi da quelli degli ordinari. Questa relazione si concentra dunque proprio su questi aspetti. Naturalmente, essendo la sicurezza un concetto unitario, coinvolgente dunque anche minacce quali la criminalità organizzata interna e transnazionale e il terrorismo, si tratterà anche di tali profili, laddove direttamente incidenti sulla materia.

1. Le caratteristiche della minaccia attuale

La minaccia del terrorismo jihadista si è trasformata sensibilmente negli ultimi anni e pone quindi sfide in parte nuove[1]. Conoscere l'oggetto delle indagini è necessario per diverse ragioni. Innanzitutto solo questa approfondita conoscenza consente di adeguare gli strumenti e le tecniche investigative alle esigenze specifiche. Questo vale per ogni indagine ma è ancora più importante quando il singolo fatto-reato è inserito in una catena di eventi, in un contesto storico-politico che ne fornisce la chiave interpretativa. Quando poi, come nel caso del terrorismo, la risposta giudiziaria è solo una parte del complesso delle misure di contrasto, tra le quali anche politiche mirate ad eradicarne le ragioni profonde, conoscere e comprendere diviene addirittura vitale.

Le norme incriminatrici e quelle che fondano l'utilizzo degli strumenti processuali mi sembrano oggi molto efficaci. Ne vedremo subito alcune applicazioni nel campo delle *intercettazioni*. Premetto che questo termine, che continuerò ad usare per brevità, rappresenta invece solo una parte delle potenzialità di azione che sono attribuite agli organi di investigazione e a quelli di prevenzione e sicurezza nel settore delle comunicazioni. In realtà vi sono potenzialità molto diversificate, che vanno dalla captazione di conversazioni alla perquisizione informatica a distanza e al conseguente sequestro fino alla intromissione, anche "offensiva", nei dispositivi o nei siti web.

La magistratura italiana e le strutture investigative che da essa dipendono hanno maturato negli anni di un lungo contrasto del terrorismo interno e di quello internazionale, operante nel Paese, la consapevolezza della necessità di rispetto delle garanzie fondamentali della persona come precondizione *anche* dell'efficacia dell'intervento repressivo. Se vi sono state pressioni dell'opinione pubblica, a volte recepite dal legislatore, perché si abbandonasse la strada diritta delle garanzie, è stata l'interpretazione attenta dei p.m. prima e dei giudici poi a costituire un baluardo, che ha svuotato di reale offensività anche quei conati di legislazione d'emergenza.

1 Il primo paragrafo costituisce sintesi e rielaborazione del mio scritto *Conoscere il Terrorismo Jihadista. Strumenti e tecniche di indagine.* Relazione al seminario di Pisa dell'11 marzo 2016, in *Questione Giustizia on line*

Abbiamo tutti, magistrati impegnati su questo terreno e forze di polizia, ben chiari i limiti che la Costituzione ci pone e siamo ben attrezzati a respingere, già nelle nostre coscienze, qualunque approccio di diritto penale del nemico o di coinvolgimento del giudice nella "lotta" ai fenomeni.

Dunque, non si tratta di anticipare ancora la soglia delle condotte punibili. Lo strumentario è già adeguato ed anzi va interpretato con cura alla luce di quei principi appena ricordati. Del resto la Corte di Cassazione si dimostra assai attenta e costituisce per tutti noi una guida insostituibile. Neppure si tratta di immaginare nuovi strumenti investigativi. Anche questi sono adeguati.

Vi sono però alcuni aspetti, strettamente correlati all'oggetto del nostro incontro, che devono essere affrontati. Saranno necessarie probabilmente alcune misure di rafforzamento delle capacità di captazione e di intervento sul web e bisognerà meglio tarare i rapporti tra repressione e raccolta di dati provenienti dalla intelligence. Ma nulla che stravolga l'approccio che abbiamo seguito sin qui, con risultati così positivi.

Per comprendere la necessità di questi nuovi strumenti è indispensabile anche adeguare il nostro armamentario interpretativo.

Conoscere i fondamenti ideali delle organizzazioni terroristiche è indispensabile innanzitutto per una corretta applicazione delle norme. Si eviterà così da un lato di estendere oltre il dovuto e il necessario l'area della investigazione, spingendo settori di mero antagonismo verso scelte più radicali; dall'altro lato si cercherà di colpire condotte particolarmente offensive, per il contesto in cui esse effettivamente si inseriscono, e che invece possono apparire meno significative se quel contesto non si comprende. Inoltre gli strumenti investigativi potranno essere tarati sulle specifiche esigenze del settore, adattandosi alle modalità operative delle organizzazioni terroristiche, nella loro attuale realtà.

La comprensione profonda delle radici del fenomeno è ancora più importante se si considera che l'uso del metodo terroristico è in sé in grado di condizionare fortemente le scelte individuali e collettive; da questo il terrorismo trae il suo nome e la sua forza. Si pensi a come la mera prospettazione, sin qui priva di supporto nei fatti e dunque falsa, di un legame tra migranti e terrorismo[2] abbia contribuito a legittimare scelte politiche gravissime per l'idea stessa di Europa, fino a mettere in discussione il pilastro della libera circolazione delle persone nei suoi confini, per comprendere quanto la possibile successione di gravi attentati possa incidere sulle libertà di noi tutti.

Pericolo tanto più grande se si considera la trasformazione che si è andata verificando nel fronte del terrorismo internazionale[3].

2 Le uniche emergenze procedimentali sono costituite dallo sfruttamento a fini di finanziamento della tratta dei migranti, o attraverso il taglieggiamento delle stesse organizzazioni di trafficanti oppure attraverso il controllo di alcune delle reti, che sembrerebbe risultare da recenti acquisizioni; questo rischio era peraltro stato ben previsto da tempo, come evidenziato più volte dalla Procura di Catania, anche con riferimento alle modificazioni politiche libiche. Evidente è anche la probabilità, anzi la certezza, che tra le decine di migliaia di migranti che entrano nel territorio dello Stato provenendo da zone di conflitto, molti siano già radicalizzati e possano quindi costituire terreno di reclutamento. Non risulta invece che il canale dei migranti via mare nel Canale di Sicilia sia stato utilizzato per far entrare in Europa combattenti addestrati.

3 Rinvio ai miei scritti *Ciò che non dobbiamo imparare dall'America*, *Limes*, febbraio 2007 e *Une alternative à la "guerre contre le terrorisme". L'experience italienne*, *Esprit, 2007*

Non è facile sintetizzare le caratteristiche, in parte del tutto nuove e in parte già esistenti, delle recenti manifestazioni del terrorismo islamico; esse vanno riconsiderate nel contesto della più generale trasformazione. Darò quindi per scontate alcune premesse, che forse non lo sono.

La principale novità è costituita dalla fondazione territoriale di alcune organizzazioni, che rivendicano l'inizio della costruzione di un nuovo califfato. Questa fondazione non ha nulla a che vedere con rivendicazioni etniche o nazionali. Nulla a che vedere con la volontà di avere una propria terra, dove far crescere le radici di un popolo, identificato per tradizioni, costumi, lingua, religione. Tutto ciò è dietro le spalle, almeno nella percezione di sé che hanno alcune organizzazioni terroristiche e i loro militanti. Anzi, il rifiuto dell'Islam basato sulla consuetudine, sull'adattamento dei precetti alle situazioni locali, etniche, storiche, è parte integrante e fondamentale dell'ideologia jihadista[4]. Questa impostazione ha una chiara radice anticolonialista, nel rifiuto della costruzione di confini tracciati con la squadra sulle carte geografiche (si veda il gesto simbolico dell'abbattimento del confine Siria- Iraq da parte di ISIS). Essa ha però una molto più profonda radice nel carattere tendenzialmente universale della comunità musulmana, che – almeno nella sua visione millenaristica – non ha confini se non quelli definiti dalla effettiva presenza della comunità stessa. Il califfato è espressione politica di questa concezione. Non è un'arma propagandistica e non è una ridicola sceneggiata. E' un richiamo a un messaggio politico-religioso ben presente alla comunità musulmana, i cui saggi non hanno mai smesso di studiare e di farne oggetto di polemiche interne, spesso feroci, con gravi conseguenze per chi ha ne ha messo in dubbio la riferibilità al messaggio del Profeta[5].

Il fatto che non vi sia più una diretta connessione con una singola zona di conflitto (ad esempio, in passato, l'Afghanistan, la Cecenia, la Serbia ecc.) ha enfatizzato e reso del tutto diversa sul piano qualitativo la caratteristica già esistente della internazionalizzazione del reclutamento.

Ciò determina l'ulteriore effetto della autonomia della motivazione politico-religiosa, rispetto ad altri aspetti, che pure restano fondamentali nelle motivazioni collettive e individuali.

Nella Jihad universale si intrecciano anticolonialsmo, disillusione politica, radicalizzazione religiosa, in una miscela nella quale le predicazioni salafiste radicali ridefiniscono le frontiere del bene e del male e rendono lecito e moralmente doveroso l'assassinio del miscredente.

In altre parole, non è che gli aspetti relativi alle radici sociali e politiche in senso stretto dell'adesione alla scelta estrema siano irrilevanti. Al contrario, esse rimangono di grande importanza. Quelle radici però si vestono di una più generale ideologia, in grado di reclutare soggetti con le più diverse motivazioni personali, fornendo una solida cornice "narrativa". Il messaggio del ritorno alla purezza dell'Islam delle

4" Si veda, sul punto del revivalismo islamico (*Islamism, fundamentalism, Wahabbism*) e sulla sua opposizione al *Customary Islam* la ricca introduzione di C. Kurzman a *Liberal Islam. A sourcebook*, Oxford University Press, 1998.

5 Tra i tantissimi esempi, anche recenti, mi sembra utile citare un eminente studioso di scienza islamica, Abd al Raziq, autore nel 1925 di uno scritto fondamentale sul Califfato, ora tradotto in spagnolo (*El Islam y los fundamentos del poder*, Universidad de Granada, 2007) e leggibile in estratto in un importante volume, che raccoglie scritti dei più rilevanti esponenti dell'Islam moderato, secondo una selezione interna e dunque non con occhi "occidentali", a cura e con ampia introduzione di Charles Kurzman, *Liberl Islam,* citato. Per avere sostenuto un'interpretazione del Califfato che portava alla separazione tra Stato e religione (*Islam, una religione, non uno Stato*) fu allontanato dall'Università Al Azhar dove insegnava e accusato di eresia. Cito questo esempio perché mi sembra indicativo della profondità e della vicinanza temporale del dibattito, interno all'Islam, sul Califfato, anche dopo la sua soppressione da parte di Ataturk il 3 marzo 1924.

origini, come antidoto alla mancanza di valori del mondo moderno, ha una forte attrattiva sia su coloro che si sentono – e sono – emarginati, sia su chi emarginato non è affatto.

Le motivazioni di ordine sociale e politico sono quindi molto importanti e devono essere sempre tenute presenti. Ad esempio, finché il vicino oriente resterà una polveriera a causa della irrisolta questione palestinese vi sarà sempre spazio per la violenza e per il ricorso all'arma tipica del conflitto asimmetrico.

L'elemento differenziale odierno è però il ruolo molto più marcato e autonomo del messaggio religioso[6], inteso come richiamo all'attuazione della società islamica ideale, nella lettura ormai consolidatasi in larghe parti della comunità musulmana e che non consente distinzione tra religione e politica, tra scelte morali e obblighi di condotta di vita, sanzionati dalla forza o dello Stato o dei correligionari. Se coloro che passano all'azione sono un'infima minoranza, essi sono il frutto di un più vasto movimento salafita, la cui reale diffusione ci è forse ignota.

Gli elementi che caratterizzano la fase attuale del terrorismo Jihadista possono essere sintetizzati come maggiore autonomia della motivazione religiosa universale rispetto ai particolarismi legati a situazioni locali; l'esistenza di organizzazioni di riferimento con basi territoriali che si pongono come entità statali; il ricorso, che consegue da questi due elementi, a modalità di rapporti che non richiedono più complesse reti organizzative gerarchiche; l'utilizzo di strumenti di comunicazione e informatici, spesso non accessibili alle intercettazioni; uno schema *reticolare*[7] che attrae i giovani musulmani europei

L'atomizzazione della rete di contatti, resa possibile anche dal collante ideologico, il reclutamento attraverso forme diverse di avvicinamento alla comunità e di costruzione di identità condivise, la relazione continua tra reclutamento e teatri di conflitti all'estero sono tutti elementi che comportano la necessità di utilizzare strumenti di indagine adeguati alla nuova realtà.

La maggior parte delle comunicazioni interne alla rete avviene utilizzando i più diversi sistemi oggi messi a disposizione dal web e dai dispositivi di connessione. Da una parte vi sono i *social networks*, utilizzabili per i primi contatti e la radicalizzazione e poi per le comunicazioni criptate che essi consentono; altre forme di comunicazioni criptate, come Skype e WhatsApp, forniscono un'ulteriore strumento di grande diffusione; le comunicazioni satellitari consentono il mantenimento dei rapporti anche in zone di difficile copertura ordinaria. Internet è poi una fonte importantissima di diffusione del messaggio e di reclutamento, anche attraverso l'utilizzo di strumenti come i video-giochi[8]. Le grandi fonti di finanziamento provenienti dallo sfruttamento delle risorse dei territori controllati e la fondazione di uno stato in fieri, rendono possibile la creazione di vere e proprie strutture di tipo aziendale per la gestione della propaganda e delle reti.

6 Questo aspetto era già stato evidenziato da uno dei massimi esperti del terrorismo internazionale, che però condivide solo in parte l'impostazione di chi scrive. Si veda Armando Spataro, *Cosa induce tante persone ad abbracciare il terrorismo? Perché si diventa terroristi ? Le esperienze di un Pubblico Ministero.* In *Voci contro l barbarie- La battaglia per i diritti umani attraverso i suoi protagonisti,* a cura di Antonio Cassese, Feltrinelli (novembre 2008)

7 Teorizzato da Abu Musab al-Suri, *Appello alla resistenza islamica mondiale*, gennaio 2005, che – secondo G. Kepel, *Terreur dans l'Hexagone. Genèse du Djihad Francais,* Gallimard, 2015, p.52 – avrebbe avuto un ruolo decisivo nella trasformazione dell'islamismo radicale francese, sostituendo all'attacco al "nemico lontano" e quindi all'organizzazione piramidale di al-Quaida, priva di radici sociali, "un jihadismo di prossimità, secondo un sistema reticolare penetrante alla base, e non più al vertice, le società nemiche da abbattere".

Un secondo aspetto rilevante per l'oggetto della nostra analisi è costituito dalla provenienza delle informazioni necessarie per penetrare nelle organizzazioni terroriste, anche ai fini della repressione penale. Una parte consistente delle attività illecite si svolge infatti in territori sottratti al controllo di altre entità statali o in zone di conflitto aperto. Ciò rende impossibile il ricorso ai tradizionali strumenti di cooperazione giudiziaria o di polizia. La grande importanza delle informazioni raccolte anche in zone di conflitto rende poi necessario riflettere su come assicurare agli interlocutori la segretezza delle fonti e delle metodologie utilizzate, realizzando un bilanciamento tra questa esigenza e quella repressiva.

Anche la prevenzione deve essere condotta nell'assoluta legalità. Essa non è terra di nessuno e incognita: *hic sunt leones*.

2. Gli strumenti a disposizione in materia di intercettazioni e di interferenza

Da quanto sin qui detto appare evidente l'importanza del tema della accessibilità da parte dell'autorità giudiziaria e delle Agenzie di Informazione a tutte le forme di comunicazione, anche quelle per le quali attualmente si presentano invece gravi problemi, anche di sovranità nazionale.

Cerchiamo quindi di focalizzare i punti di maggiore rilevanza che emergono dalle caratteristiche in parte nuove del terrorismo di matrice islamica.

In primo luogo si conferma, rispetto alle esperienze già maturate nel campo della criminalità organizzata, la centralità dell'acquisizione delle informazioni che possono essere acquisite con le forme di intercettazione di comunicazioni e di flussi telematici.

Anzi, questa centralità è resa ancora più significativa per:

- Il ricorso abituale a comunicazioni criptate di vario genere (whatsapp; skype; ecc.)
- La riduzione all'essenziale delle strutture organizzative e il ricorso sistematico a comunicazioni via web
- L'utilizzo di ogni forma di comunicazione web per l'avvicinamento, il reclutamento, l'indicazione in termini generali delle modalità operative ecc.
- L'esistenza di aree territoriali da cui operano strutture in grado di elaborare e porre in essere le misure e le contromisure che consentono di attuare l'utilizzo delle comunicazioni web
- La possibilità di uso offensivo delle capacità di cui al punto che precede (hakeraggio; penetrazione ecc.)

Tralascio in questa sede le intercettazioni convenzionali, essendo esse ben note nei presupposti, nelle modalità di autorizzazione e nell'utilizzabilità delle acquisizioni. Tra queste intercettazioni tradizionali pongo anche quelle relative alle comunicazioni satellitari. Queste infatti non sono concettualmente diverse da quelle telefoniche o di flussi telematici. Il problema è oggi costituito dalla mancanza di collaborazione da

8 Ho potuto, a ragione del mio lavoro, vedere un agghiacciante video, diffuso in rete, nel quale veniva replicato un video gioco, realizzato però con persone reali, in cui un gruppo di ragazzini di circa 10-12 anni, di diversa provenienza, erano impegnati nella ricerca e nell'uccisione di ostaggi, con difficoltà sempre crescenti e in un ambiente (i resti di un'antica città) molto simile a quello di tanti video giochi. Il ragazzino che completava il gioco scoprendo l'ultimo ostaggio aveva il privilegio-premio di decapitarlo.

parte dei gestori, situati all'estero e ai quali non possono – al momento – essere imposte prestazioni obbligatorie. Vi sono sistemi di intercettazione che però sono di assai difficile realizzazione tecnica e sui quali non mi soffermo.

Anche le intercettazioni di comunicazioni tra presenti, c.d. ambientali, non pongono in sé problemi diversi da quelli che abitualmente affrontiamo in tema di regimi differenziati, di presupposti ecc. Può forse qui accennarsi al tema della diversità di disciplina a livello internazionale, per il davvero singolare caso del Regno Unito, nel quale non è possibile fare alcun uso processuale delle intercettazioni telefoniche (anche se autorizzate ai fini del procedimento e in tal caso avranno mera valenza investigativa), mentre sono ammissibili in corte quelle ambientali.

2.1 Il virus

Un metodo per intercettare comunicazioni è costituito dalla inoculazione di un *virus*, generalmente detto *Trojan*, abbreviazione di *Trojan Horse*. Ve ne sono di varie specie e origine. Essi funzionano venendo installati nel dispositivo da controllare o mediante accesso diretto o mediante una comunicazione nascosta che contiene il programma aggressivo. Il dispositivo può essere costituito da qualunque strumento atto alla comunicazione o alla captazione di informazioni dall'ambiente vicino; si può trattare di un computer, di un tablet, di un telefono ecc.. Il virus deve essere calibrato sul tipo di dispositivo e spesso vi sono periodi di tempo in cui il rilascio di nuove versioni o aggiornamenti nel software o nell'antivirus, rendono impossibile l'installazione, fino a che anche il nuovo programma non viene craccato.

Una volta installato il virus agisce trasmettendo all'operatore le informazioni. Vi sono diverse tipologie di programmi virus, che operano con modalità differenti e con diversa efficacia, ma per quello che ci riguarda è sufficiente notare che un dispositivo aggredito dal virus viene trasformato in un terminale lontano dell'operatore che ne ha il controllo (*backdoors*).

Esso può quindi funzionare captando le comunicazioni che avvengono nell'ambiente e dar luogo così a una intercettazione "tra presenti", non diversa da quella che ha luogo con un dispositivo fisso. Le comunicazioni captate vengono poi trasmesse con varie modalità e processate dall'operatore come qualunque altra intercettazione da lontano.

Il primo elemento che distingue l'intercettazione effettuata con il virus è costituita dal fatto che il dispositivo può essere mobile; non sempre, in quanto esso può essere installato anche su di un dispositivo fisso, come un computer, ma in genere si tratterà di un cellulare, di un tablet, di un portatile ecc.. Se installato su dispositivo mobile, la captazione seguirà il dispositivo. Essa dunque avverrà – se effettuata in continuità - in un numero non predeterminabile di luoghi, tra cui è possibile ve ne siano anche di privata dimora. Il dispositivo "posseduto" può essere utilizzato per captare anche le immagini, ponendosi in questo caso i problemi giuridici noti in tema di immagini a contenuto comunicativo, le sole che possono essere legittimamente utilizzate.

La modalità operativa del dispositivo "posseduto" ha posto il quesito della legittimità di un'intercettazione nella quale il luogo sia incerto. Ci torneremo tra breve, non prima di aver chiarito che in realtà la captazione di comunicazioni (suoni) è solo una delle potenzialità del virus.

Esso funziona anche come captatore delle comunicazioni che si svolgono *per mezzo* del dispositivo. Se esso funzionerà come un telefono, il virus trasformerà il dispositivo in un mezzo di intecettazione telefonica.

Questo punto è fondamentale perché al momento il virus è l'unico strumento in grado di captare le conversazioni criptate, dopo la decriptazione.

Molte applicazioni di uso comune si avvalgono della criptazione, che avviene in origine e alla fine della comunicazione, con sistemi diversi a seconda del produttore dello strumento ma che hanno in comune l'impossibilità di avere le chiavi di entrata e di uscita, che non sono in possesso di coloro che comunicano. Ciò rende la comunicazione non intercettabile. Questa caratteristica è molto apprezzata da una tipologia di utenti che vuole evitare l'ascolto ed è infatti addirittura propagandata dal gestore negli avvisi pubblicitari.

L'esperienza ci insegna che questi metodi di comunicazione criptati (WhatsApp; Skype ecc.) sono utilizzati anche dai membri delle organizzazioni terroristiche per le ordinarie comunicazioni. E' dunque di fondamentale importanza poterle acquisire.

L'acquisizione avviene mediante la captazione della comunicazione subito dopo la decriptazione, quando giunge sul dispositivo, oppure subito prima nel caso di comunicazione in uscita.

Si tratta di captazione di comunicazioni, perfettamente rientrante nel concetto di intercettazione quale disciplinato dal codice di rito, anche se essa avviene mediante l'acquisizione di un contenuto estratto dalla conversazione vera e propria.

E bene sottolineare ciò perché il virus è in grado di invadere ogni parte del dispositivo e dunque di acquisire ogni tipo di informazione in esso contenuta, si tratti di immagini, documenti, messaggi ecc.. Essa realizza cioè una sorta di perquisizione informatica, cui segue l'apprensione del contenuto (e cioè il suo sequestro).

Presupposti (meno stringenti) e trattazione procedimentale dell'atto (con tempi di discovery più breve) differiscono e creano un non piccolo problema giuridico.

Poiché il virus, in alcune sue strutturazioni, pervade l'intero dispositivo, esso consente anche operazioni "offensive", dalla distruzione o alla sostituzione di files, all'invio di comunicazioni, all'installazione di programmi ulteriori e così via. Anche questa, come appresso si vedrà, ha una potenziale utilità per le azioni di contrasto del terrorismo, ma fuoriesce dal concetto di intercettazione per quanto largo e giunge in campi dei quali parleremo tra breve.

2.2 La legittimità del virus

Le Sezioni Unite della Corte di Cassazione decideranno (o avranno già deciso, al momento in cui questo intervento sarà discusso[9]) una questione posta dalla VI Sezione penale.

Il collegio, ravvisando un potenziale contrasto con la sentenza n. n. 27100/15 del 26.6.2015 della stessa Sezione, ha rimesso la questione alle Sezioni Unite della Corte di cassazione e, a conclusione di una approfondita motivazione della sua ordinanza (Cass., Sez. VI, ord. n. 59 del 10/3/2016 in proc. n. 13884/16), ha sintetizzato le questioni da sottoporre alle Sezioni Unite nei seguenti termini:

9 In data 29 maggio 2016 la Corte di Cassazione ha diffuso un'informazione provvisoria, dalla quale risulta che è stata riconosciuta la legittimità delle intercettazioni mediante virus, limitatamente a procedimenti relativi a delitti di criminalità organizzata, anche terroristica, nonché quelli comunque facenti capo a un'associazione per delinquere.

- *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 dove debba avvenire la relativa captazione;*
- *se, in mancanza di tale indicazione, la eventuale sanzione di inutilizzabilità riguardi in concreto solo le captazioni che avvengano in luoghi di privata dimora al di fuori dei presupposti indicati dall'art. 266, comma 2, c.p.p.;*
- *se possa comunque prescindersi da tale indicazione nel caso in cui l'intercettazione per mezzo di virus informatico sia disposta in un procedimento relativo a delitti di criminalità organizzata.*

Al di là dei quesiti oggetto di potenziale contrasto, è possibile che la Corte affronti ex professo l'intera materia dell'impiego di software di spywares nell'ambito del procedimento penale. Non è certo questa la sede per approfondire la questione, sulla quale peraltro la Procura Generale è intervenuta in giudizio con una completa e molto interessante memoria, che allego alla mia relazione con il consenso dell'estensore, l'Avvocato Generale Nello Rossi, che l'ha redatta con la collaborazione di un gruppo di sostituti procuratori generali e che l'ha discussa insieme al s.procuratore Antonio Balsamo.

Ciò che conta qui mettere in rilevo è che lo strumento si è dimostrato di straordinaria importanza nelle indagini di criminalità organizzata di stampo mafioso e lo sarà ancor più in quelle in materia di terrorismo, per le ragioni che ho innanzi cercato di evidenziare. In secondo luogo, notazione non meno importante, è possibile differenziare l'impiego del software in maniera tale da assicurare il rispetto delle garanzie che presidiano la riservatezza della vita privata e in particolare quella area che attiene alla nostra "personalità informatica", la cui aggressione deve avvenire solo con un attentato bilanciamento dei contrapposti interessi di rilievo costituzionali.

La Corte Costituzionale federale tedesca ebbe modo di occuparsi della legittimità della modifica della Legge di protezione della Costituzione del *Land* del Nord Reno-Westfalia (2006), che consentiva l'utilizzo di *spywares* per la sorveglianza *on line* da parte di un organismo di *intelligence* a "protezione della Costituzione" (*Verfassungsschutzbehörde*), afferente al Ministero dell'Interno.

La sentenza del 27 febbraio 2008, nel dichiarare incostituzionale la disposizione, ha seguito un percorso argomentativo fondato non sulla tutela dei diritti costituzionali sanciti dalla Carta (segretezza delle comunicazioni, art. 10; inviolabilità del domicilio, art. 13) ma sul contrasto tra l'attività di *intelligence* (la ricerca a distanza dei dati contenuti su dispositivi digitali) rispetto ad un nuovo diritto fondamentale, che tutela il cittadino digitale nell'uso delle tecnologie di informazione e di comunicazione in rete.

Ritenuta insufficiente la protezione offerta dagli artt. 10 e 13 della Costituzione federale, la Corte ha affermato l'esistenza di un nuovo diritto costituzionale alla riservatezza ed alla integrità dei sistemi informatici. Così come il diritto all'autodeterminazione informativa, questo nuovo diritto fondamentale viene fatto derivare dall'art. 1.1 della legge fondamentale, il quale dispone che "la dignità umana è inviolabile e tutti gli organi dello Stato hanno l'obiettivo finale di proteggerla".

Secondo la Corte, il ricorso a nuove forme di investigazione tecnologica non è di per sé contrario alla Costituzione. Tuttavia, la loro regolamentazione, a livello legislativo, e la loro utilizzazione, a livello esecutivo, non possono non tener conto del bilanciamento con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo. Questo si traduce, per il legislatore, a livello di tecnica normativa, nell'obbligo del rispetto dei principi di chiarezza e sufficiente determinatezza della fattispecie, del principio di proporzionalità. La possibilità di effettuare un accesso segreto è dunque costituzionalmente ammissibile solo se tale misura risulta essere necessaria per la protezione di importanti e predominanti beni giuridici,

quali possono essere la vita, l'incolumità fisica e la libertà dei singoli, nonché quelli della collettività, la cui minaccia tocca le fondamenta dello Stato o il suo mantenimento o la base dell'esistenza umana, fino a comprendere anche la possibilità di funzionamento delle parti essenziali dei servizi di pubblica utilità.

Un punto fondamentale della motivazione riguarda la riserva della decisione all'autorità giudiziaria. Le attività di indagine in esame, infatti, devono essere controbilanciate da idonee precauzioni procedurali, riservando la misura ad un ordine del giudice che svolga un controllo preventivo, che dovrebbe avere la funzione di "compensazione di rappresentanza" degli interessi della persona interessata al procedimento.

La declaratoria di incostituzionalità non ha riguardato, pertanto, i nuovi mezzi "di carattere tecnologico" in quanto tali ed in termini assoluti, ma i loro modi di utilizzo, i presupposti ed i limiti, anche temporali, per la loro adozione[10].

I requisiti di proporzionalità e specificità sono richiesti anche dalla legge spagnola, come condizione di legittimità del provvedimento autorizzatorio, demandato al giudice.

In Spagna è stata recentemente approvata la Legge Organica 13/2015 di modifica della Legge di Procedura Penale per il rafforzamento delle garanzie processuali e la regolamentazione degli strumenti di indagine tecnologica[11], tra cui anche la captazione di comunicazioni orali a mezzo di dispositivi.

Sul punto, nel preambolo[12] si afferma innanzitutto che il ricorso a tali strumenti si è rivelato indispensabile e che richiedeva pertanto un'espressa regolamentazione, che seguisse alcune idee chiave: la prima, l'attribuzione della decisione al giudice[13]; la seconda, il rispetto dei principi di specialità, eccezionalità,

10 Questi e gli atri riferimenti comparati in tema di *spywares* sono tratti dalla memoria preparatoria per la discussione dinanzi alle Sezioni Unite, redatta dalla Procura Generale della Corte di Cassazione, che è allegata alla presente relazione.

11 *Ley Orgánica 13/2015, de modificación de la Ley de Enjuiciamiento Criminal para el fortalecimiento de las garantías procesales y la regulación de las medidas de investigación tecnológica*. La traduzione dei brani della legge è mia e può essere imprecisa.

12 "*La experiencia demuestra que, en la investigación de determinados delitos, la captación y grabación de comunicaciones orales abiertas mediante el empleo de dispositivos electrónicos puede resultar indispensable. Se trata de una materia hasta ahora ausente de la regulación del proceso penal y cuyo alcance se aborda con sujeción a dos ideas clave. La primera, la exigencia de que sea el juez de instrucción el que legitime el acto de injerencia; la segunda, la necesidad de que los principios rectores de especialidad, excepcionalidad, idoneidad, necesidad y proporcionalidad actúen como elementos de justificación de la medida. Esta medida solo podrá acordarse para encuentros concretos que vaya a mantener el investigado, debiéndose identificar con precisión el lugar o dependencias sometidos a vigilancia. Por tanto, no caben autorizaciones de captación y grabación de conversaciones orales de carácter general o indiscriminadas, y, en consecuencia, el dispositivo de escucha y, en su caso, las cámaras a él asociadas, deberán desactivarse tan pronto finalice la conversación cuya captación fue permitida, como se desprende del artículo 588 quater c.*"

13 Nei casi di urgenza nella materia del terrorismo il potere di autorizzare l'intercettazione in questione è però attributo al Ministro dell'Interno dall'art. 588 ter d; il provvedimento urgente è soggetto da convalida giudiziale.

idoneità, necessità e proporzinalità.Inoltre l'utilizzo dello strumento di captazione potrà essere utilizzato solo in luighi determinati, escludendosi autorizzazioni di carattere generale o indiscriminato.

Al fine di assicurare il rispetto di queste ultime limitazioni, l'art. 588 ter d prevede in generale una precisa identificazione dei dispositivi, delle connessioni, della disponibilità degli stessi da parte di soggetti determinati, nonchè tra l'altro la conoscenza dell'origine e della destinazione della comunicazione captata al momento in cui essa ha luogo, con la precisazione della posizione geografica di tali punti.

Per ciò che concerne specificamente l'utilizzo di strumenti elettronici per la captazione di conversazione nell'ambiente gli artt. 588 quater e aggiungono ulteriori requisiti di specificità e necessità, tra i quali la finalizzazione solo a determinate categorie di reati, tra cui quelli di terrorismo. Lo strumento di captazione delle comunicazioni della persona oggetto dell'investigazione può essere posto in luoghi pubblici o aperti, nella casa o in ogni altro luogo chiuso.

Ulteriori previsioni disciplinano il caso di impiego di programmi, installati segretamente sui dispositivi dell'indagato, per l'esame da remoto del contenuto (perquisizione da remoto). Viene ampliato dagli artt. 588 septies a e ss. il quadro dei reati che consentono l'accesso, ricomprendendovisi reati come quelli contro i minori, nei quali lo strumento informatico è particolarmente importante, nonché i reati contro la Costituzione e gli interessi fondamentali dello Stato (tradimento e difesa nazionale).

Tra le misure di cautela addizionali vanno segnalati l'obbligo di preservare l'integrità del computer e dei dati in esso contenuti e la necessità di un ulteriore, specifico provvedimento di autorizzazione per la copia del contenuto.

Anche la Francia consente l'accesso segreto ai dati di ogni genere esistenti nelle memorie o transitanti in via informatica nei dispositivi di persone sottoposte alle indagini per una vasta categoria di reati, su ordine dell'autorità giudiziaria. Questa parte della normativa è tuttavia al momento oggetto di modifiche legislative.

In conclusione sul punto, non è necessario sacrificare uno strumento di assoluta importanza, addirittura non sostituibile per la captazione di comunicazioni centrali nei procedimenti per fatti di terrorismo e per le attività di prevenzione. Le esigenze di tutela dei diritti del cittadino possono infatti essere conseguite differenziando le modalità operative del virus. Il p.m. e il giudice dovranno essere ben attenti nel disciplinarle nel momento dell'autorizzazione, distinguendo ciò che è autorizzato da ciò che non lo è.

L'utilizzo di un monitoraggio di localizzazione può contribuire ad attenuare i rischi per la privacy di terzi, consentono la captazione solo in luoghi predeterminati o escludendone altri. Le potenzialità diverse dalla captazione devono poi trovare rispondenza nella disciplina dei diversi istituti. Ad esempio, può essere inibito l'accesso ai dati (perquisizione e sequestro) o limitato ad alcune tipologie e può essere effettuato il sequestro solo al termine delle operazioni, in modo da effettuare nei termini il prescritto deposito.

2.3 Le intercettazioni preventive delle Forze di Polizia

L' art. 266 disp. att. c.p.p. attribuisce al Ministro dell'Interno o, su sua delega, ad alcune autorità della Polizia di Stato, dei Carabinieri e della Guardia di Finanza, il potere di effettuare intercettazioni preventive di comunicazioni. La norma ha subito nel tempo alcuni interventi, volti ad estenderne l'ambito di applicazione anche alla prevenzione del terrorismo, oltre che dei gravi delitti di criminalità organizzata. La struttura delle operazioni è analoga alla disciplina delle ordinarie intercettazioni a fini processuali. Esse sono però autorizzate dal pubblico ministero distrettuale e non dal giudice ed è fatto divieto assoluto di utilizzo nel

processo. La rivelazione del contenuto delle captazioni è punito quale delitto.

Le informazioni raccolte potranno essere utilizzate per finalità preventive e dunque per conoscere approfonditamente i fenomeni in atto e per impedire che si portino a conclusione condotte illecite in fase preparatoria. Inoltre esse saranno utilizzate come notizia di reato e in questi limiti potranno avere utilizzo procedimentale.

In materia di terrorismo, le intercettazioni preventive:

- sono possibili quando siano necessarie per l'acquisizione di notizie concernenti la prevenzione dei delitti di cui all'art. 407 comma 2, lett. A) n. 5 cpp (cioè "*delitti commessi per finalità di terrorismo o di eversione dell'ordine costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui all'art. 270, terzo comma e 306, secondo comma, del Codice Penale")*
- possono riguardare non solo le conversazioni-comunicazioni telefoniche, ma anche quelle cd. *ambientali* e quelle per via telematica (oltre che l'acquisizione dei tabulati telefonici e telematici).

Le intercettazioni preventive sono conosciute da molti stati europei, in larga parte attraverso autorizzazione del ministro competente o di un suo delegato, senza intervento dell'autorità giudiziaria. Esse sono assimilate a quelle effettuate dai Servizi e dalle Agenzie di Informazione.

2.4 Le intercettazioni delle Agenzie di Informazione

Nel nostro Paese le Agenzie di Informazione e Sicurezza possono effettuare intercettazioni di comunicazioni ed acquisire tabulati telefonici e telematici[14].

Anche queste intercettazioni sono sottoposte ad autorizzazione giudiziaria, per la quale è competente il Procuratore generale di Roma. Originariamente si era prevista l'attribuzione del potere di autorizzazione a tutti i Procuratori generali ma questa diffusione è apparsa in contrasto sia con le esigenze di segretezza che con la necessità di un controllo che rispondesse a criteri uniforme e fosse – proprio per la concentrazione delle informazioni sui precedenti e sulle prassi – maggiormente autorevole. L'art. 12 co. 1 della legge n. 133/2012 ne previde quindi la concentrazione in capo alla sola Procura generale della capitale[15].

Pur richiamandosi, per la parte procedurale, l'art. 226 disp. att. c.p.p., in realtà le intercettazioni dei servizi differiscono profondamente dalle intercettazioni preventive delle forze di polizia.

Il circuito che porta all'autorizzazione, infatti, vede al centro il Presidente del Consiglio e dunque l'Autorità Nazionale per la Sicurezza, cui compete di vagliare la proposta dei direttore delle Agenzie, tramitata dal direttore del DIS (Dipartimento Informazioni per la Sicurezza). L'ANS valuta quindi la sussistenza dei presupposti che legittimano l'intercettazione e che sono stati nel 2012 estesi a ricomprendere tutti i settori attività delle Agenzie di informazione.

14 Decreto-legge 27.7.2005 n. 144 (cd. "Decreto Pisanu"), convertito con Legge 31 luglio 2005 n. 155

15" Legge 7 agosto 2012, n. 133, Modifiche alla legge 3 agosto 2007, n. 124 , concernente il Sistema di informazione per la sicurezza della Repubblica e la disciplina del segreto.

Una volta esauritasi la fase di competenza dell'autorità giudiziaria, la procedura ritorna al controllo demandato all'autorità politica e il circuito si chiude nel Comitato Parlamentare (COPASIR).

All'autorità politica spetta la valutazione della sussistenza dell'interesse nazionale mentre al procuratore generale il controllo, oltre che sull'effettiva esistenza di tale presupposto sulla base dei fatti esposti nella richiesta di autorizzazione, anche di parametri non normativamente definiti ma desumibili dall'essenza stessa del controllo giurisdizionale, anche qui sulla base della prospettazione del richiedente: pertinenza, stretta necessità, proporzionalità. Il procuratore generale controlla anche che al termine delle operazioni i materiale raccolto sia integralmente distrutto, della qual cosa deve essergli data comunicazione scritta in un tempo assai breve. Questa misura è volta a rendere effettiva la destinazione delle informazioni raccolta alla sola attività istituzionale delle Agenzie e a prevenire rischi di disseminazione del materiale captato.

Originariamente le intercettazioni potevano riguardare solo la raccolta di informazioni riguardanti criminalità organizzata e terrorismo. La legge del 2012 (art. 12) ha esteso l'area di ammissibilità a tutte le attività demandate alle Agenzie dagli articoli 6 e 7 della legge 3 agosto 2007, n. 124.

All'Agenzia informazioni e sicurezza esterna (AISE) è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili alla difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica, anche in attuazione di accordi internazionali, dalle minacce provenienti dall'estero. Essa inoltre pone in essere le attività in materia di controproliferazione concernenti i materiali strategici, nonché le attività di informazione per la sicurezza, che si svolgono al di fuori del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia. È, altresì, compito dell'AISE individuare e contrastare al di fuori del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

All'Agenzia informazioni e sicurezza interna (AISI) è affidato il compito di ricercare ed elaborare nei settori di competenza tutte le informazioni utili a difendere, anche in attuazione di accordi internazionali, la sicurezza interna della Repubblica e le istituzioni democratiche poste dalla Costituzione a suo fondamento da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica Inoltre spettano all'AISI le attività di informazione per la sicurezza, che si svolgono all'interno del territorio nazionale, a protezione degli interessi politici, militari, economici, scientifici e industriali dell'Italia. È, altresì, compito dell'AISI individuare e contrastare all'interno del territorio nazionale le attività di spionaggio dirette contro l'Italia e le attività volte a danneggiare gli interessi nazionali.

Quindi le attività di intercettazione potranno riguardare non solo la prevenzione dei delitti di criminalità organizzata e di terrorismo, ma il più ampio campo delle diverse attribuzioni delle Agenzie, dal controspionaggio alla tutela di interessi fondamentali dello Stato, come individuati dalla legge.

Anzi, alcuni di questi settori sono proprio quelli più vicini alla logica tradizionale dei servizi segreti, dal controspionaggio alla tutela dei settori strategici quali la difesa nazionale, le infrastrutture strategiche ecc.

Nel campo della prevenzione del terrorismo le intercettazioni delle Agenzie potrebbero avere una grande efficacia, in quanto esse potrebbero – unitamente ad altri strumenti – dare corpo alle informazioni raccolte all'estero e che necessariamente sfuggono alla possibilità della cooperazione giudiziaria o di polizia, riversandole in attività che possano poi avere un effettivo utilizzo sia di prevenzione che, ricorrendone i presupposti, ai fini della punizione dei responsabili.

Questa attività, così come quella in materia di criminalità organizzata, rischia di interferire con le attività giudiziarie, anche per il contesto istituzionale italiano, che vede il pubblico ministero e la polizia giudiziaria

concentrare la maggior mole di informazioni e il più ampio strumentario investigativo, a differenza di altri Paesi. La collaborazione costante tra il Procuratore generale e il Procuratore Nazionale Antimafia, presso cui convergono tutti i dati esterni delle intercettazioni, consente di evitare o di porre rimedio a queste interferenze, con soluzioni di volta in volta concordate anche con i Procuratori distrettuali.

Credo che la scelta di non attribuire al PNA il potere di autorizzare queste intercettazioni e di assegnarlo invece ad un organo più lontano dalle investigazioni, quale è il procuratore generale d'appello, abbia avuto il senso di mantenere netta la distinzione tra le due differenti strade della giurisdizione e della prevenzione attraverso i Servizi, assicurando la prevenzione di sempre possibili contaminazioni, deleterie per l'una come per gli altri.

Non vi è omogeneità nei Paesi europei circa l'organizzazione dei Servizi e circa i poteri di intercettazione agli stessi attribuiti. In questo campo è stato molto importante il ruolo giocato dalla Convenzione Europea dei Diritti dell' Uomo e dai Trattati. In linea generale, si richiede che l'interferenza con la vita privata e la raccolta e trattazione dei dati raccolti debbano avvenire in un contesto definito dalla legge e ben specificato dalle norme regolamentari. Le decisioni della Corte di Strasburgo[16] hanno indicato, in una serie di casi, i livelli minimi di garanzia che la legge deve apprestare per esser considerata idonea a soddisfare i requisiti della Convenzione. Questi sono essenzialmente, oltre alla definizione da parte della legge delle autorità cui il potere è conferito e dell'ampiezza e limiti della conseguente discrezionalità, la natura della minaccia; la definizione delle categorie di soggetti che possono essere obiettivo dell'intercettazione; le procedure da seguire per esaminare, utilizzare e conservare i dati ottenuti; le precauzioni nel trasmettere a terzi le informazioni; casi e modalità di eliminazione dei dati.

Questo livello minimo di garanzie (*quality of the law*) deve essere assicurato in tutti i casi di sorveglianza elettronica[17].

Un ruolo importante svolgono il Garante Europeo per la protezione dei dati e le corrispondenti autorità nazionali, nel configurare un quadro di riferimento. Molto diversificate sono invece le procedure di autorizzazione preventiva e di controllo successivo.

Non è richiesto che le intercettazioni siano autorizzate dall'autorità giudiziaria. Ciò avviene in molti paesi ma non in tutti i Paesi europei. Autorità responsabili possono essere anche il ministro (dell'interno o degli esteri) o il presidente del consiglio/primo ministro; vi sono anche casi in cui è richiesto l'intervento di comitati di esperti.

Recenti rivelazioni, come il caso Snowden, oltre ad aver dato luogo a decisioni giudiziarie che vedremo tra breve, hanno determinato interventi legislativi che hanno rafforzato le garanzie.

2.5 Le attività sottocopertura. In particolare quella sui siti Internet

Le caratteristiche peculiari del terrorismo più recente di matrice islamica rendono molto importanti le attività sottocopertura, in quanto in grado di sopperire – attraverso i contatti personali – alla mancanza di strutture organizzative di tipo tradizionale e di avvicinare così l'organizzazione reticolare.

Un aspetto centrale di questo genere di attività è costituito dall'utilizzo dei contatti web per raccogliere

16 In particolare, *Weber and Saravia v. Germany, 2006* e *Liberty and Others v. United Kingdom, 2008,* su cui oltre.

17 *Liberty*, citata

informazioni e impedire le condotte illecite in atto. Mai queste attività dovrebbero sconfinare nella provocazione o nell'istigazione a commettere reati, anche se il confine con quest'ultimo aspetto può a volte essere labile. E infatti evidente che l'agente sotto copertura deve accreditarsi come soggetto affidabile per essere reclutato e dunque fungere da contatto e magari svolgere a sua volta attività di apparente reclutamento. Le attività di questo genere, nell'ambito dei servizi di informazione, si legano strettamente al tema delle garanzie funzionali, cioè di quella complessa procedura volta ad autorizzare e quindi rendere legittime condotte che altrimenti sarebbero punibili. Il circuito di autorizzazione è tutto interno a quello che fa capo alla responsabilità politica del Presidente del Consiglio.

Le attività sotto copertura possono essere condotte anche dalle forze di polizia specializzate per lo svolgimento dei compiti loro attribuiti e dunque per la prevenzione e la repressione di gravi reati.

L'art. 4, c. 2 del D.L. n. 374/2001, conv. nella L. 438/2001 prevede che gli ufficiali ed agenti di Polizia giudiziaria specializzati, al fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo anche internazionale, possono utilizzare indicazioni e documenti di copertura anche per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone il pubblico ministero entro le 48 ore successive all'inizio delle attività.

L'esecuzione di tali operazioni è disposta, secondo l'appartenenza del personale di Polizia giudiziaria, dal Capo della Polizia di Stato o dal Comandante generale dell'Arma dei Carabinieri o della Guardia di Finanza per le attribuzioni inerenti ai propri compiti istituzionali, ovvero, per loro delega, rispettivamente dal Questore o dal responsabile di livello provinciale dell'organismo di appartenenza, ai quali deve essere data immediata comunicazione dell'esito della operazione.

L'organo che dispone l'esecuzione dell'operazione, inoltre, deve dare preventiva comunicazione al pubblico ministero competente per le indagini, indicando, quando richiesto, anche il nominativo dell'ufficiale di Polizia giudiziaria responsabile dell'operazione. Il pubblico ministero deve essere informato altresì dei risultati dell'operazione.

Con l'art. 7 bis, c. 2 del cd. "Decreto Pisanu" n. 144/2005 (conv. nella L. n. 155 del 31.7.05), si è poi previsto che, per la prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo condotte con i mezzi informatici, le stesse operazioni sotto copertura, così come le intercettazioni preventive, possano essere effettuate anche dagli ufficiali di polizia giudiziaria appartenenti all' "organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione", la c.d. Polizia Postale e delle Telecomunicazioni.

Questo organismo opera con grande professionalità; esso ha ottenuto risultati straordinari in campi diversi, che vanno dalla pedopornografia al gioco clandestino on line, all'assistenza agli organi di polizia nel settore della criminalità organizzata. E' dunque da ritenersi che anche in materia di terrorismo internazionale sarà possibile ottenere buoni risultati.

La legge 16/03/2006 n° 146 di ratifica della convenzione delle Nazioni Unite contro il crimine organizzato transnazionale, prevede le attività sottocopertura per il contrasto del crimine transnazionale. Per quanto qui di specifico rilievo, va evidenziato che l'art. 9 prevede che gli ufficiali di polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato e dell'Arma dei carabinieri specializzati nell'attività di contrasto al terrorismo e all'eversione e del Corpo della guardia di finanza competenti nelle attività di

contrasto al finanziamento del terrorismo, possano, nel corso di specifiche operazioni di polizia e, comunque, al solo fine di acquisire elementi di prova in ordine ai delitti commessi con finalità di terrorismo, anche per interposta persona, e dunque avvalendosi di ausiliari, compiere attività che sarebbero altrimenti punibili. Queste sono così indicate: "danno rifugio o comunque prestano assistenza agli associati, acquistano, ricevono, sostituiscono od occultano denaro, armi, documenti, stupefacenti, beni ovvero cose che sono oggetto, prodotto, profitto o mezzo per commettere il reato o altrimenti ostacolano l'individuazione della loro provenienza o ne consentono l'impiego".

Entro i limiti sopra indicati, i reparti specializzati possono utilizzare documenti, identità o indicazioni di copertura per attivare o entrare in contatto con soggetti e siti nelle reti di comunicazione, informandone il pubblico ministero al più presto e, comunque, non oltre 48 ore dall'inizio delle attività per indagini antiterrorismo, nonché tenendolo al corrente dello svolgimento e dei risultati delle operazioni.

E' molto importante notare che la legge autorizza anche l'attivazione di siti nelle reti, la realizzazione e gestione di aree di comunicazione o scambio su reti o sistemi informatici, secondo le modalità stabilite con decreto del Ministro dell'interno, di concerto con il Ministro della giustizia e con gli altri Ministri interessati.

2.6 Le attività offensive. Il WEB profondo

Occorre aver sempre ben chiaro che anche le organizzazioni criminali si adeguano alle capacità di detezione delle forze deputate al loro contrasto. Anzi, lo fanno con grande rapidità, in questo aiutate dal fatto che le aziende che commercializzano prodotti di vario genere non si fanno scrupolo a investire risorse notevolissime nel realizzare strumenti atti ad evitare le intromissioni e addirittura pubblicizzano i loro prodotti anche con questo valore aggiunto.

Un esempio è quello della criptazione delle comunicazioni o dei dispositivi. Si ricorderà la vicenda che ha visto contrapposti Google (che si è riparata dietro il rispetto della riservatezza…) e FBI. Essa si è risolta quando l'Agenzia statunitense ha comunque craccato la protezione, spendendo circa un milione e mezzo di dollari in hackeraggio (fonti di stampa confermate).

Esempio ancora più allarmante è la sostituzione dell'ormai ben noto Web profondo, *Deep Web,* quali *Tor*, e similari, con una nuova rete invisibile, *Internet Invisible Project- I2P,* a cui si accede scaricando un programma esistente su Internet, e che costituisce al momento una sfida di grande pericolosità. La rete invisibile opera con lo stesso meccanismo, quindi essenzialmente su rapporti *peer to peer*, ed assicura al momento assoluta anonimità.

Si comprende quindi quanto sia importante che il Legislatore abbia ora introdotto[18] la possibilità di azioni "offensive", in grado di contrastare l'utilizzo del web da parte delle organizzazioni terroriste. E dunque ora espressamente previsto che l'autorità giudiziaria (dunque anche il pubblico ministero) possa disporre che i siti inseriti in un elenco predisposto dal Ministri dell'Interno, utilizzati per le attività e le condotte di cui agli articoli 270-bis e 270-sexies del codice penale, siano rimossi. Il pubblico ministero può emettere il provvedimento motivato quando si procede per i delitti di cui agli articoli 270-bis,270-ter, 270-quater e

18" Art. 2 del decreto legge 18 febbraio 2015 n. 7, convertito con modificazioni dalla L. 17 aprile 2015, n. 43. Nel provvedimento legislativo si prevedono anche aggravanti quando i reati sono commessi avvalendosi di mezzi telematici.

270-quinquies del codice penale commessi con le finalità di terrorismo di cui all'articolo 270-sexies del codice penale, e sussistono concreti elementi che consentano di ritenere che si compiano dette attività per via telematica.

Nei giorni scorsi gli Stati Uniti hanno reso noto l'impiego di potenti strumenti di colonizzazione delle reti con l'impianto di virus e l'hackeraggio, come forma di contrasto del terrorismo ISIS[19]. La rivelazione, affermano fonti della NSA, sarebbe parte della guerra psicologica nei confronti della dirigenza ISIS, che diverrebbe incerta circa il reale contenuto delle comunicazioni oggetto della manipolazione. Obiettivo della cybercampagna è "di disgregare la capacità dello Stato Islamico di diffondere il proprio messaggio, di attrarre nuovi aderenti, di trasmettere ordini nella catena di commando e di svolgere le azioni quotidiane, come pagare i combattenti". Le poche anticipazioni fornite indicano alcune modalità operative, certamente non le sole. Dopo avere a lungo monitorato le comunicazioni e averne appreso tipologia e modalità[20], si dovrebbe ora passare alla fase "offensiva" di manipolazione dei messaggi, con lo scopo – tra l'altro – di determinare reazioni quale lo spostamento dei militanti in aree più vulnerabili.

L'utilizzo di questi strumenti è facilitato, dal punto di vista giuridico e della loro legittimità, dal fatto che si rivolgano a un territorio in questo momento privo di sovranità e nei confronti di un'entità che ha pretesa di rappresentarsi come stato. Le questioni legali sono state a lungo discusse, per limitare i profili di interferenza con attività di terzi o legali, ma sono state superate sulla base della considerazione che ISIS ha "utilizzato il cyberspace unicamente per reclutare, per comunicare attraverso applicazioni cifrate e per coordinare le azioni in Europa".

Campo in parte nuovo, sul quale occorrerà che anche in Italia vengano assunte chiare determinazioni su legittimità, presupposti, modalità e limiti.

Nettamente distinte dalle intercettazioni preventive e dalle attività volte a contrastare l'uso del web sono le intercettazioni generalizzate, a strascico (c.d. phising, termine utilizzato anche per le truffe on line), anche quando utilizzino filtri sofisticati. Questo genere di intercettazioni senza mandato dell'autorità giudiziaria sono state ampiamente utilizzate da alcuni Paesi.

Sono ormai di dominio pubblico le attività di captazione globale effettuate da alcuni stati, con enormi potenzialità di ascolto e di interferenza. Negli Stati Uniti, dopo una serie di scandali[21], si è giunti nel 2015 al USA FREEDOM Act, che ha revisionato alcuni aspetti del PATRIOT Act nella parte relativa alla raccolta

19 New York Times, Dvid E. Sanger, U.S. Unleashes Digital Arsenal in War With ISIS, 24/25 aprile 2016

20 Ricordo che già nelle indagini per l'attentato ai danni del professore Massimo D'Antona il gruppo di lavoro della Procura di Roma cercò di costruire un programma, avvalendosi di tecnici della Polizia ed esterni, in grado di individuare la "impronta telematica", ricavata da una serie di indici, in grado di identificare l'utilizzare di un dispositivo. Le risorse limitate non consentirono un esito positivo. In compenso un buon lavoro di indagine, connesso all'impiego di sofisticati software realizzati appositamente, consentì l'individuazione della carta telefonica usa e getta, e – addirittura – il sequestro della carta utilizzata per alcune delle chiamate di rivendicazione: come ritrovare il gettone, un risultato straordinario.

21 Si veda ad esempio la rivelazione nel 2005 da parte del New York Times del programma di intercettazioni segrete Terrorist Surveillance Program, TSP, e più recentemente il caso Snowden, che ha reso pubblico il massiccio programma di sorveglianza PRISM.

massiva di metadati, ripristinando il ruolo dell'organo giurisdizionale, *Foreign Intelligence Surveillance Court* (FISC), o dell'*Attorney General* in caso di urgenza[22]. Tuttavia restano programmi di acquisizione massiva di dati internet e comunicativi, mentre è posto in questione anche il ruolo svolto effettivamente dal FISC, anche attraverso la regolamentazione delle procedure.

In Gran Bretagna si è reso necessario un giudizio dinanzi al Tribunale per i poteri investigativi (IPT, su cui oltre) e poi un secondo giudizio di chiarificazione del primo, dopo pochi mesi, sui programmi PRISM e UPSTREAM. Si tratta di decisioni ampiamente motivate e complesse, che qui possono essere solo rapidamente sintetizzate ma che meritano approfondimenti.

Nella prima decisione[23] il Tribunale ha fissato alcuni requisiti, rispettati i quali le attività di captazione massiva sono considerate legittime. Il tribunale fonda il suo giudizio sul necessario bilanciamento dei contrapposti interessi alla sicurezza nazionale e alla tutela dei diritti dei cittadini. Non sempre, afferma il tribunale, il Parlamento ha saputo tener dietro agli straordinari progressi della tecnologia, cosicché si è potuto da qualcuno sostenere che i servizi segreti abbiano avuto in questo settore *carta* bianca. Ma, afferma il tribunale, non è così, almeno per gli aspetti ad esso sottoposti: "La legge dà agli individui adeguate indicazioni sulle circostanze e le condizioni per le quali gli Intelligence Services sono legittimati a ricorrere alle intercettazioni o a farne uso".

Queste sono, in sintesi, le condizioni:

i) Non può essere fatto alcun uso di questo genere di intercettazioni all'estero per aggirare i divieti interni
ii) Devono essere applicati i criteri della stretta necessità e della proporzionalità rispetto agli interessi definiti dalla legge (sicurezza nazionale rispetto a terrorismo o a gravi crimini; interessi economici della nazione)
iii) Il materiale raccolto può essere conservato solo nei limiti e fino a quando necessario e deve poi essere distrutto
iv) I Servizi sono considerati responsabili per la correttezza nell'operato e devono tenere delle operazioni adeguata documentazione, al fine di consentire il controllo delle autorità a ciò deputate.

Il Tribunale ha dunque "salvato" PRISM e UPSTREAM ma ha da un lato posto paletti rigorosi, dall'altro ha inteso indirizzare un monito al legislatore per una più accurata disciplina, mantenendo aperta la possibilità di un ulteriore approfondimento[24]

Questo secondo round ha avuto luogo il 6 febbraio 2015, con quello che il Tribunale definisce "secondo giudizio". Questa volta il tribunale ha dichiarato che prima del giudizio del 2014 le attività di captazione,

22 Secondo l'uso statunitense, il titolo è un acronimo per ***U****niting and* ***S****trengthening* ***A****merica by* ***F****ulfilling* ***R****ights and* ***E****nding* ***E****avesdropping,* ***D****ragnet-collection and* ***O****nline* ***M****onitoring Act*. Entreremmo in un discorso troppo vasto per questa relazione se affrontassimo le tematiche statunitensi. Chi è interessato può tuttavia trovare un'ampia informazione per gli aspetti relativi alla nuova disciplina della raccolta dei metadati nella relazione della National Security Agency (NSA), *Transparency report: The USA FREEDOM Act Business Record FISA,* che può essere letta nel sito NSA.

23 Liberty, Privacy International e altri v. The Secretary of State and GCHQ e altri, resa il 5 dicembre 2014.

conservazione e trasmissione di comunicazioni private erano in violazione degli artt. 8 e 10 CEDU ma che la corrente disciplina aveva posto rimedio alle violazioni.

Va poi aggiunto che erano state considerate legittime le operazioni di intercettazione di comunicazioni tra la Gran Bretagna e l'estero, operate sulla base di filtri (operazioni ora apparentemente abbandonate, almeno nella forma che fu resa nota, sia per le polemiche cui diedero luogo, sia perché non risulta che abbiano avuto esiti positivi). Il Tribunale specializzato del Regno Unito, investito della questione[25], ritenne che le specificazioni contenute nel provvedimento di autorizzazione emesso dal segretario di Stato, le misure atte a impedire la disseminazione delle informazioni, la distruzione delle stesse e il divieto di copia, il divieto di utilizzo nelle corti ecc. fossero idonei a garantire il bilanciamento necessario tra l'interesse perseguito e la riservatezza delle comunicazioni.

Peraltro le attività di ascolto indiscriminato di un numero elevatissimo di comunicazioni, oltre a porre seri problemi di legittimità anche laddove non è espressamente prevista l'autorizzazione giudiziaria, sono a mio parere inutili perché non in grado di fornire informazioni effettivamente gestibili, anche quando vengono usati filtri sofisticati.

3. Le difficoltà nelle relazioni tra gli Stati europei in questo settore.

Il legame, nelle forme che si sono viste, tra soggetti radicalizzati che vivono e operano in Europa e tra questi e i loro referenti all'estero e in zone di conflitto, rende necessario l'utilizzo di informazioni che provengono da aree territoriali nelle quali non vi è possibilità di cooperazione giudiziaria o di polizia.

E dunque di fondamentale importanza l'utilizzo di informazioni raccolte in attività di *intelligence*. Queste sono, in larga parte e per definizione, segrete e tali devono restare per ragioni di protezione delle fonti o delle modalità operative.

Quando le informazioni devono essere utilizzate in un procedimento penale, si pone il problema della forma in cui possono essere acquisite e del bilanciamento tra l'esigenza punitiva e quella di tutela del segreto.

Inoltre, il carattere diffuso – delocalizzato – delle organizzazioni reticolari del terrorismo islamico attuale, rende ancora più importante la cooperazione tra Stati.

Questa cooperazione è resa molto difficile non solo dalla diversità di previsioni legali in termini di reati e di strumenti processuali, ma molto più in profondità dalle differenze ordinamentali, istituzionali e di mentalità (prassi istituzionali, ad esempio).

24 "161. This has been a valuable exercise, in which, with the benefit of full and penetrating advocacy on all sides, the Tribunal has been enabled to carry out a review of the systems in relation to both Prism and/or Upstream and the s.8(4) warrant. We have been able (as we state in paragraph 156) to satisfy ourselves that as of today there is no contravention of Articles 8 or 10 by reference to those systems. As set out in paragraphs 153 and 154 above, we have left open for further argument the question as to whether prior hereto there has been such breach. We shall also proceed, guided by the submissions we have heard and the conclusions we have reached, to consider in closed whether there has been in fact any unlawful interception or treatment of the Claimants' communications".

25 IPT 2004. Sul Tribunale, si veda oltre.

Partiamo da quest'ultimo punto. Molto è stato fatto per rendere compatibili gli ordinamenti penali nell'Unione e nella Comunità internazionale in genere. Vi sono però ancora differenze di fondo.

Per restare al campo limitato del nostro intervento, una prima differenza tra ordinamenti è data dal ruolo e dall'inserimento nella rete delle istituzioni del pubblico ministero. Il p.m. italiano, a differenza di quello di molti altri paesi, è autorità giudiziaria. Ciò si riflette sulla possibilità che esso emetta provvedimenti direttamente incidenti su diritti costituzionalmente tutelati (limitazione della libertà, ispezioni, perquisizioni, sequestri, intercettazioni); la legge ordinaria disciplina poi le modalità di esercizio di questi poteri.

Il riflesso immediato nel campo delle intercettazioni di vario genere è che esso – a differenza di altri analoghi organi – potrebbe emettere provvedimenti complessi, di cui appresso si parlerà.

Le peculiari caratteristiche del p.m. italiano, legate al principio costituzionale di obbligatorietà dell'azione e alle conseguenze che se ne traggono in tema di direzione delle indagini e della polizia di giudiziaria e dei rapporti con altri poteri dello Stato, si riflettono anche sulla titolarità del potere di disporre le intercettazioni e altre forme di accesso a sfere riservate della vita della persona, e sulla finalizzazione di questi accessi al processo.

In altri ordinamenti vi è una netta scissione tra questi aspetti, con la conseguenza che questo genere di attività è condiviso da diverse fonti di autorizzazione e ha finalità ben distinte.

E' dunque molto difficile comparare i sistemi complessi di governo della intromissione nella vita privata. Vi sono ancora differenza fondamentali e alcuni Paesi non rendono note in maniera completa le capacità di intercettazione e le modalità concrete con le quali esse vengono gestite.

Le finalità di prevenzione e di tutela della sicurezza dello Stato comportano poi la dislocazione di tali poteri verso organi non giudiziari e con modalità non finalizzate alla esternazione delle informazioni acquisite.

Quando l'intercettazione è finalizzata al processo penale, la sua stessa esistenza e il contenuto sono segreti solo ai fini e nei limiti delle necessità procedimentali. Il segreto è funzionalmente volto a realizzare quegli obiettivi e dura solo per il tempo e nell'estensione necessari a perseguirli. L'intercettazione disposta per finalità preventive o di sicurezza dello Stato è per sua natura segreta sia nell'esistenza che nei risultati; il segreto tendenzialmente non è destinato a cessare se non per ragioni di tutela di interessi che gli ordinamenti ritengono di bilanciare e che a un certo punto possono prendere prevalenza (ad esempio, tutela della privacy o del circuito di controllo).

La questione è oggi molto calda in Italia, tanto che alcune Procure della Repubblica hanno emanato direttive finalizzate a trovare, nelle pieghe della disciplina, possibilità interpretative che riducano il pericolo di trasmigrazione di informazioni riservate e non utili all'accertamento dei reati[26]. La prima, per quanto mi è noto, fu emessa dalla Procura di Catania il 24 aprile 2012 e riguardava specificamente il tema delle

26 Direttive della Procura di Napoli, Roma e Torino, in *Questione Giustizia on line*, con premessa di G.Cascini.

comunicazioni tra difensore e assistito[27]; essa fu poi da qualcuno ritenuta applicabile anche ad altri casi, come quello che riguardò le comunicazioni del Presidente della Repubblica.

I meccanismi di bilanciamento tra interessi diversi e di controllo sono profondamente diversi, anche in relazione alle regole e prassi costituzionali. Si consideri il caso della Gran Bretagna, nella quale – in un contesto che si vedrà meglio tra breve – la captazione e l'utilizzo (a fini di prevenzione) delle comunicazioni protette, anche quelle dei Parlamentari, è ampiamente consentito, salvo che le comunicazioni non concernano gli interessi protetti (ad esempio, per i MP le comunicazioni attinenti al mandato; per i ministri del culto le comunicazioni attinenti la cura delle anime; per i giornalisti, contatti con le fonti ecc.). Per il "privilegio legale" la disciplina sembra analoga a quella prevista nella direttiva della Procura di Catania, innanzi citata[28], anche se vi sono grandi differenze, dovute alla proiezione non pubblica dei risultati ottenuti e alla conseguente previsione di complessi meccanismi di controllo e salvaguardia interni al circuito.

Il diritto alla riservatezza e alla protezione dei dati personali sono protetti direttamente dagli artt. 7 e 8 della Carta Europea e dall'art.8 della CEDU; il secondo è richiamato anche nell'art. 16 del Trattato sul Funzionamento dell'Unione nell'art. 39 del Trattato dell'Unione. Questi diritti trovano tutela nella Corte di Strasburgo e in quella di Lussemburgo. Il contesto normativo è poi delimitato da decisioni quadro e da direttive. A seguito dello scandalo Snowden e della rivelazione della raccolta massiva di dati, il Parlamento Europeo ha adottato, il 12 marzo 2014, un'importante risoluzione su questo genere di programmi di sorveglianza. Tra le varie misure messe in atto dall'Unione per rendere effettivo un controllo che abbia alcune caratteristiche comuni, vi è il lavoro sistematico della Agenzia Europea per i Diritti Fondamentali. La raccolta dei dati sul funzionamento delle attività di sorveglianza dei Servizi segreti è raccolta in rapporti periodici[29], molto utili per l'esposizione delle fonti, della giurisprudenza, delle strutture in maniera comparata. La stessa Agenzia sottolinea però che la materia della sicurezza nazionale è attribuita ai singoli stati, che operano in maniere molto diverse.

---

27 La direttiva può leggersi in Archivio Penale, n.3 2012, con nota critica di F. Siracusano, *Intercettazione di colloqui tra difensore e assistito. Soluzioni 'poco convincenti che pongono in pericolo lo spazio protetto' per l'esercizio dell'attività difensiva.*

28 Si veda il paragrafo 3.3 del *Equipment Interference Code of Practice*: "Legal privilege does not apply to communications or items held with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications or items will lose their protection if there are grounds to believe, for example, that the professional legal adviser is intending to hold or use the information for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so".

29 Il rapporto *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU*, novembre 2015, può essere letto sul sito dell' Agenzia, insieme ad altro interessante materiale. L'Agenzia ha in corso attualmente una nuova verifica. Il rapporto contiene un'ampia descrizione dei diversi tipi di attività di intercettazione, sia mirata (targeted) che massiva (bulk) e con diverse modalità, a partire da quella SIGINT, di derivazione militare, relativa a qualunque tipo di emissione elettronica. L'utilizzo di metodologie SIGINT non è consentita in Italia su bersagli nazionali.

Queste radicali diversità rendono molto difficile il dialogo e lo scambio delle informazioni raccolte e la loro effettiva utilizzabilità ai fini processuali.

Questa considerazione ci porta al secondo punto.

I servizi e le agenzie di informazione (e anche le polizie quando operano in funzione della sicurezza dello Stato) tendono ad operare con modalità basate essenzialmente sul riconoscimento reciproco. In questo contesto "comunitario" un ruolo fondamentale è giocato dalla fiducia. Innanzitutto ogni struttura considera preminente l'interesse del proprio Paese; esse rispondono al circuito di responsabilità nazionale e in un regime di segretezza; spesso le operazioni di spionaggio e controspionaggio sono rivolte verso gli stessi Paesi "amici"; la protezione delle fonti (considerate proprietà e spesso frutto di un duro e costoso lavoro) e delle modalità e capacità operative (anch'esse frutto di impegno, a volte enorme) è considerata prioritaria.

Ogni disvelamento non concordato di questi aspetti operativi o dei risultati ottenuti è considerato una grave violazione del rapporto fiduciario. Di conseguenza è visto con sospetto ogni sistema nel quale le informazioni ottenute sono destinate a una segretezza solo provvisoria, ad esempio per l'utilizzo nel processo penale in forma pubblica (vi sono Stati nei quali è consentita la forma realmente segreta – non limitata quindi al nostro dibattimento a porte chiuse – di acquisizione di alcune tipologie di informazioni). Analoga protezione è data alle informazioni ad alto contenuto di confidenzialità, come quelle mediche o di orientamento spirituale.

Nel nostro ordinamento non è consentito far uso di qualunque genere delle informazioni raccolte e dunque nemmeno a fini processuali. E' da escludersi che possa essere ammessa qualunque forma di utilizzo "segreto" delle informazioni, come avvenuto in altri ordinamenti, con grave danno per i diritti fondamentali e per la tenuta stessa della Costituzione democratica. Sul punto rinvio ai miei scritti già citati. Semmai occorre chiedersi se sia ancora attuale il divieto di apporre il segreto[30] sulle informazioni che riguardino, tra l'altro, "fatti di terrorismo o eversivi dell'ordine costituzionale" (art. 11 della legge 124/2007). A seguito dell'estensione del concetto di "terrorismo" anche a quello di carattere internazionale, la norma renderebbe impossibile tutelare adeguatamente le fonti e le metodologie impiegate nella ricerca, soprattutto quando in collaborazione con altri organismi. Tra l'altro, la previsione appena citata si riflette anche sulle garanzie funzionali, che consentivano attività protette solo nella ipotesi di cui al secondo comma dell'art. 270bis c.p, e cioè alla partecipazione ad organizzazione con finalità di terrorismo. Ora il Legislatore è intervenuto, estendendo l'eccezione alle fattispecie di cui agli articoli 270, secondo comma, 270-ter, 270-quater, 270-quater.1, 270-quinquies, 302, 306, secondo comma, e 414, quarto comma, del codice penale[31].

Nonostante quest'ultima previsione lasci immutati i termini di inapponibilità del segreto di Stato, intervenendo solo sulle garanzie funzionali, credo che sia possibile interpretare la norma che vieta l'apposizione del segreto (con i conseguenti obblighi di comunicazione all'autorità giudiziaria delle

30 Sulla differenza concettuale tra apposizione e opposizione del segreto rinvio al mio scritto, *Il segreto di Stato tra responsabilità politica e controllo giurisdizionale,* in *Raccolta di scritti in onore di Loris D'Ambrosio, Quaderno d'Intelligence,* n.3, Roma, p. 25 ss.

31 Art. 8 del decreto legge 18 febbraio 2015 n. 7, convertito con modificazioni dalla L. 17 aprile 2015, n. 43

informazioni raccolte, derivante dalla norma di chiusura di cui all'art. 23 della legge 124/2007[32]) nel senso della sua originaria funzione, di impedire condotte illecite dei servizi segreti, finalizzate a destabilizzare l'ordine costituzionale, e soprattutto di impedirne la copertura per mezzo del segreto. Purtroppo i fatti recenti che hanno visto più Presidenti del Consiglio opporre all'autorità giudiziaria il segreto in maniera che ha trovato conforto in discusse decisioni della Corte costituzionale[33], rende oggi difficile parlare di questo aspetto, per sospetti incrociati che subito si attivano, ma il danno che può venire alla sicurezza nazionale dalla inaffidabilità della tenuta del segreto potrebbe essere davvero significativo.

Un Paese che ha sempre tenuto in grande considerazione il diritto a un processo equo (dobbiamo alla tradizione anglosassone i concetti stessi di *due process of law* e di *fair trail*, tradotti come "giusto processo") e allo stesso tempo la tutela degli interessi superiori dello Stato, anche attraverso il segreto, ha trovato un bilanciamento[34] che da noi non sarebbe forse oggi possibile, a causa della formulazione rigida dell'art. 111 della Costituzione (diffidate sempre delle imitazioni!). Si tornerà tra breve su aspetti che riguardano

---

32 L'art. 23 prevede, al comma 7 che "**i** direttori dei servizi di informazione per la sicurezza e il direttore generale del DIS hanno l'obbligo di fornire ai competenti organi di polizia giudiziaria le informazioni e gli elementi di prova relativamente a fatti configurabili come reati, di cui sia stata acquisita conoscenza nell'ambito delle strutture che da essi rispettivamente dipendono". Secondo il comma 8 tale adempimento può essere solo ritardato, e mai omesso, "su autorizzazione del Presidente del Consiglio dei ministri, quando ciò sia strettamente necessario al perseguimento delle finalità istituzionali del Sistema di informazione per la sicurezza".

33 Rinvio ai miei scritti, con riferimenti bibliografici e di giurisprudenza: *La Corte e il Segreto di Stato*, in *Cassazione Penale,* ottobre 2009; *Processo penale e Segreto di Stato. Oltre Abu Omar*, in *Questione Giustizia,* n. 2/2010

34 Sally Cullen, magistrato di collegamento britannico in Italia, in una relazione tenuta a Scandicci il 18 settembre 2015 ha sintetizzato efficacemente i termini del bilanciamento, che prevede obblighi di *discovery*, temperati dalla necessità di rispettare il segreto, anche sulle fonti e particolarmente quando queste provengono da organismi esteri; in questo caso il giudice, anche in assenza del difensore e a richiesta del p.m., valuta la possibilità di utilizzare le informazioni mantenendo riservata la fonte o – se ciò non è possibile – se e come il processo possa proseguire. Poiché la relazione non è accessibile, ne trascrivo qui la parte di rilievo:
"I procuratori hanno l'obbligo di divulgare agli imputati qualsiasi materiale in proprio possesso (o in possesso degli investigatori) che non intendono utilizzare come prova, ma che o mette a rischio l'esercizio dell'azione penale o potrebbe altrimenti essere di ausilio all'imputato nella preparazione del caso (es. prove a discarico).
Hanno inoltre l'obbligo (anche se con un margine di considerazione) di ottenere tale materiale dai paesi stranieri *(R v Akbar Alibhai and Others (2004)).*
Qualsiasi agenzia in possesso di materiale pertinente inutilizzato predisporrà o una tabella del materiale o prenderà contatto con il procuratore e li inviterà ad ispezionare tale materiale.
Perché il materiale risulti sensibile in tale contesto occorre che la sua divulgazione implichi un reale rischio di grave pregiudizio ad un importante interesse pubblico. Tale materiale viene di norma catalogato come Materiale la cui immunità è di interesse pubblico (PII). Nel caso in cui il procuratore concordi con il fatto che qualsiasi materiale PII soddisfa il test di divulgazione, questi insieme con la agenzia competente deve valutare se sia possibile pubblicare il materiale in maniera tale che non risulti più sensibile. In tale caso verrà aggiunto alla tabella del materiale non-sensibile e sarà divulgato alla difesa ed al tribunale.
Nel caso in cui il materiale catalogato come *PII* non può essere pubblicato allora il procuratore deve valutare se l'imputato potrebbe ancora avere un giusto processo senza la divulgazione del materiale. Questo potrebbe implicare la presentazione del caso su determinate basi o mediante la scelta di non basarsi su altro materiale, ammissibile.
Nel caso in cui ciò sia possibile allora l'accusa deve comunicare al giudice del processo l'esistenza di materiale *PII* e richiedere il consenso di procedure su tale base. Questo avviene nell'ambito di un'udienza *PII* che potrebbe aver luogo in uno dei tre modi, stabilito dalla delicatezza del materiale *PII (Rule 25 CPR- Criminal Procedure Rules).*

specificamente le intercettazioni ma preme qui sottolineare che porre il problema è necessario e non ci fa iscrivere nella zona della lavagna destinata ai cattivi.

Il settore delle intercettazioni è particolarmente sensibile in questo senso. Le capacità tecniche di intercettazione sono spesso considerate da proteggere. E' dunque molto difficile operare giudizi comparati che siano fondati su fatti realmente noti. Ad esempio, è ormai opinione consolidata, difficilmente contrastabile anche a livello europeo, che l'Italia sia il Paese delle intercettazioni. Ciò dipende dal fatto che la quasi totalità delle intercettazioni è emessa nel nostro Paese nell'ambito del processo penale o a fini di prova o di prevenzione (in entrambe i casi attraverso l'utilizzo di registri i cui numeri sono accessibili); in molti altri Paesi non vi è la limitazione costituzionale che prevede l'autorizzazione della autorità giudiziaria

---

- 'Tipo 1' (*inter partes*). La difesa viene avvisata dell'udienza e viene comunicato in linea generale che tipo di materiale *PII* esiste. Gli viene data la possibilità di rivolgersi al giudice e poi di ritirarsi dall'udienza prima che il giudice ascolti l'accusa e valuti il materiale.
- 'Tipo 2' (*ex parte con avviso*). La difesa viene informata dell'udienza, ma non ha diritto a conoscere la categoria del materiale o di rivolgersi al giudice.
- 'Tipo 3' (*ex parte senza avviso*). Se il materiale *PII* è particolarmente sensibile – ovvero implica rischi per la sicurezza nazionale o l'incolumità delle persone – allora l'udienza può aver luogo senza inviare avviso alla difesa o senza che il caso risulti iscritto nel registro del tribunale.

Il Giudice deve esaminare il materiale catalogato come *PII* e decidere se il processo può continuare equamente sulle basi di quanto suggerito dall'accusa. Le richieste di *PII* relative a materiale appartenente alle agenzie di *intelligence* devono essere corredate da un certificato firmato dal Segretario di Stato competente.

Il Paese estero può specificare le modalità di utilizzo delle proprie informazioni subordinandone l'uso a determinate condizioni. Qualora per la richiesta si renda necessaria un'udienza di *PII*, il giudice, all'atto della valutazione degli elementi relativi all'interesse pubblico, terrà conto anche:

a) dell'eventualità che il rifiuto di fornire le informazioni possa fuorviare la difesa e/o impedire alla stessa di presentare un'istanza di reperimento di altro materiale escluso (per esempio perché ottenuto in cattiva fede);

b) dell'eventualità che la divulgazione delle informazioni possa avere ricadute su quanto segue:

- la capacità delle agenzia di sicurezza e di intelligence di salvaguardare la sicurezza del Regno Unito;
- la disponibilità delle fonti estere a continuare la cooperazione con le agenzie di sicurezza e di intelligence del Regno Unito oltre che con le autorità di contrasto;
- interessi economici nazionali (non già individuali o aziendali);
- la capacità da parte delle autorità di contrasto di combattere la criminalità ricorrendo all'impiego di fonti umane di intelligence segrete, operazioni sotto copertura, sorveglianza segreta ecc.;
- la salvaguardia di metodologie segrete di indagine e contrasto alla criminalità.

L'esigenza di non esporre informatori stranieri da cui provengono informazioni confidenziali è stata inoltre accolta dalle corti quale importante elemento di interesse pubblico *(R Alibhai and Others 2004 EWCA Crim 681).*

Se il giudice ritiene che non ci sia possibilità di celebrare un giusto processo senza divulgare il materiale, disporrà che abbia luogo la divulgazione. Il Procuratore procede quindi alla verifica relativa all'interesse pubblico di cui al punto 6 sopra e provvede alla divulgazione del materiale (con il consenso) ovvero, in alternativa, alla sospensione del caso.

Una volta ricevute le tabelle di materiale inutilizzato non sensibile, la difesa deve fornire una dichiarazione (*Defence Case Statement*) che illustri in termini generali la linea di difesa al fine di supportare l'accusa nella valutazione del tipo di materiale integrativo che possa risultare pertinente allo scopo di indebolire l'impianto accusatorio ovvero essere di ausilio alla difesa. *(s6 CPIA).* La difesa può inoltre scrivere alla corte chiedendo che si ordini all'accusa di divulgare il materiale aggiuntivo non utilizzato di cui sia a conoscenza in base alle tabelle ovvero di cui suppone comunque l'esistenza *(s8 CPIA).* In queste circostanze, il giudice terrà conto della pertinenza del materiale rispetto alla tesi difensiva prospettata (secondo quanto illustrato nella dichiarazione (*defence case statement*) di cui sopra) e può disporre la divulgazione. In caso di ordine di divulgazione, il procuratore deve, anche in questo caso, divulgare il materiale ovvero, in alternativa, sospendere il caso. A differenza della decisione relativa all'ammissibilità delle prove, non vi è alcun potere di impugnare un ordine di divulgazione anche se effettuato nel corso di un'udienza preparatoria *(R v H [2007] 2 W.L.R. 364 HL)".*

e vi è un contesto istituzionale che legittima altri organi ad effettuare intercettazioni senza forme di controllo pubblico (si vedrà appresso in dettaglio un esempio importante di tutela delle garanzie ottenuta in forme del tutto diverse da quella da noi vigenti), il cui numero non è noto.

Ciò porta ad una seconda conseguenza significativa, oltre a quella numerica. La finalizzazione delle intercettazioni al processo determina la loro necessaria conoscibilità, ad un certo punto del procedimento, da parte di un numero di soggetti che può essere anche molto elevato. Il contenuto informativo della captazione è poi reso disponibile in un processo pubblico, quando valutato rilevante ai fini dell'accertamento penale. E' a questo punto che si inserisce la questione, oggi molto dibattuta, della tutela della riservatezza dei terzi e degli stessi soggetti intercettati, per le parti delle comunicazioni non rilevanti.

Questa parte del problema privacy (di altra si è già detto innanzi) non è nota nelle stesse dimensioni ad altri ordinamenti perché il contenuto delle captazioni è interamente destinato a rimanere segreto. Una controprova evidente è che anche in Italia non risulta che vi siano stati problemi di violazione della riservatezza nei casi delle intercettazioni preventive o delle Agenzie di informazione e sicurezza, che pure vengono compiute ormai da molti anni e in settori sensibili.

Da quanto sin qui detto discende innanzitutto la necessità che si operi rapidamente per rende più uniformi almeno i sistemi processuali e le normative in tema di intercettazione, di accesso ai dati informatici, di utilizzazione processuale degli esiti. Deve poi restare ben chiara la distinzione tra attività a fini preventivi e di *intelligence* da quella a fini processuali, con le necessarie separazioni anche a livello istituzionale.

In attesa di un Procuratore europeo – che si avvicini però alle caratteristiche di indipendenza dai governi che ha il p.m. italiano, anche al fine di poter esercitare le funzioni di autorità giudiziaria – almeno questa disciplina è necessaria ed urgente.

4. Un caso di studio. Il Regno Unito. Il controllo del *Investigatory Powers Tribunal*.

Quanto a differenze di fondo, il Regno Unito di Gran Bretagna e Nord Irlanda è certamente un caso unico. Non si tratta solo di diversità di legislazione, struttura ordinamentale, realtà dei rapporti istituzionali. Vi è al fondo un approccio pragmatico che è difficile comprendere per chi vive al di fuori del complesso sistema relazionale su cui, alla fine dei conti, la Gran Bretagna basa davvero la sua individualità nazionale.

Mi soffermerò su di un unico aspetto, tra i tanti rilevanti nella materia in esame, perché fonte di molte informazioni utili per comprendere come sistemi diversi convergano verso risultati analoghi nello sforzo di tutelare i diritti dei singoli e gli interessi della collettività; vedremo anche, nel momento in cui non conosciamo ancora gli esiti della *Brexit*, il ruolo importante che nelle Corti UK svolgono la CEDU e la Corte Europea che della Convenzione è custode.

La Gran Bretagna conosce un utilizzo molto esteso delle intercettazioni e in genere della captazione di comunicazioni e di dati. Una parte molto piccola di questa attività è finalizzata all'accertamento di reati nel processo penale; anzi, i risultati di alcune forme di intercettazione (telefoniche) benché legittimamente autorizzate proprio per finalità di accertamento, non possono essere utilizzate a fini di prova. Anche queste attività finalizzate all'accertamento del reato non sono autorizzate dall'autorità giudiziaria ma da quella politica, che ne risponde in varie forme, anche interne (che paiono funzionare bene).

La grande maggioranza delle operazioni avviene per finalità di tutela degli interessi dell'Unione e per attività di accertamento e prevenzione, ad esempio nel campo dell'antiterrorismo.

Queste operazioni sono segrete nella loro stessa esistenza. Ancor più: la stessa capacità di svolgere tipologie determinate di captazione o di utilizzo difensivo/offensivo dell'informatica e del web è segreta. Essa emerge a volte a causa di fughe di notizie o di eventi casuali.

Tuttavia il cittadino britannico e colui che si trovi nel territorio dello Stato (le Isole) sono protetti nella loro riservatezza da alcune misure di notevole efficacia e che si basano sull'intervento di un giudice specializzato, che opera con procedure idonee a cercare di bilanciare gli interessi diversi dello Stato e dei cittadini.

Va innanzitutto chiarito che le autorità che possono svolgere sorveglianza occulta, anche attraverso la captazione di comunicazioni e le varie attività di interferenza con "proprietà", quali computers, reti ecc., sono le Agenzie di intelligence e alcune strutture di Polizia[35], sulla base di provvedimenti di autorizzazione – quando necessari – emessi dall'autorità politica (in genere il Segretario di Stato) e sottoposti a controllo nell'ambito del circuito politico (*Joint Intelligence Committee* e il comitato parlamentare *Intelligence and Security Committee*) e della stessa alta amministrazione. L' *Intelligence Services Commissioner* e l'*Interception of Communications Commissioner*, giudici di provenienza, sono nominati dal Primo Ministro e a questo rispondono, il primo con il compito di supervisionare come il Segretario di Stato emetta i *warrants* che abilitano le attività dei servizi e il secondo le attività di intercettazione; i *Commissioners* operano con incisività e la loro revisione è considerata indipendente.

Le attività sono regolate dalla legge (vi sono fonti normative diverse, che disciplinano le attività a seconda delle finalità e della autorità che opera[36]) e richiedono una valutazione di una serie di parametri non dissimili da quelli che vengono in genere riferiti alla motivazione dell'autorità giudiziaria; la valutazione è più ampia (cioè meno restrittiva) quando le operazioni riguardano l'estero ma sono legittime le medesime operazioni anche all'interno.

Il Segretario di Stato o l'autorità da questo delegata devono considerare se l'interferenza da autorizzarsi è giustificata della stretta necessità, non altrimenti ottenibile, proporzionata all'obiettivo, e abbia come fine la protezione dell'interesse alla sicurezza nazionale e alla salvaguardia degli interessi economici della GB, il prevenire o scoprire crimini gravi, dare esecuzione ad accordi internazionali di mutua assistenza in tale

35 Il Regno Unito ha tre agenzie di intelligence e sicurezza, denominate collettivamente Intelligence Services: il Secret Intelligence Service (SIS), o MI6 ("MI" sta per Military Intelligence e si occupa dell'estero); il Government Communications Headquarters (GCHQ), che è l'agenzia che si occupa specificamente della materia di cui qui ci interessiamo; il Security Service, o MI5, cui è attribuita la sicurezza interna, incluso il terrorismo. Vi sono poi altre strutture che possono raccogliere e processare informazioni, in materia di difesa (Cabinet Office, Defence Intelligence), di terrorismo (Joint Terrorism Analysis Centre), di crimine organizzato (National Crime Agency). Tutte queste agenzie devono operare entro la finalità della sicurezza nazionale, la prevenzione o scoperta dei crimini gravi, il gli interessi economici della Gran Bretagna.

36 SIS e GCHQ operano nel contesto normativo definito dal Security Service Act, 1989, Human Rights Act, 1998, dal Regulation of Investigatory Powers Act (RIPA), 2000, dall'Intelligence Services Act, 1994 (ISA).

ultimo campo. Non tutte le agenzie possono operare negli stessi campi e ad alcune è vietato operare nel territorio delle Isole.

Le attività oggetto della nostra relazione sono ora disciplinate dal Codice di condotta[37] emesso dal Segretario di Stato ai sensi della ISA e consistono in ogni tipo di "interferenza" posta in essere senza il consenso di chi ne ha diritto, operata da remoto o con altri mezzi dai Servizi di Intelligence con strumenti informatici, finalizzata a:

a) ottenere informazioni dal dispositivo;
b) ottenere informazioni sulla appartenenza, natura e uso del dispositivo;
c) localizzare ed esaminare, rimuovere, modificare, sostituire hardware o software in grado di fornire le informazioni di cui alle lettere a) e b);
d) rendere possibile e facilitare l'attività di sorveglianza attraverso il dispositivo.

Il concetto di "informazione" include il contenuto di comunicazioni e di dati delle stesse, secondo la definizione del RIPA.

Nel 2001 fu istituito un nuovo tribunale, *Investigatory Powers Tribunal (IPT)*, che giudica in unico grado sui reclami di singoli o organizzazioni in materia di interferenza in materia di comunicazioni e solo su questi aspetti. Le regole procedurali sono in parte previste dal Segretario di Stato, al fine di bilanciare le esigenze di *fair trail* con quelle del segreto[38], e in parte dallo stesso Tribunale, che le adottò nella sentenza resa in un'udienza pubblica a ciò espressamente dedicata e alla quale presero parte gli attori delle procedure in corso[39]. La regolamentazione è assai complessa e tende a bilanciare le esigenze della tutela del segreto con quelle dell'effettività della protezione da accordarsi ai reclamanti, alla luce della CEDU e della giurisprudenza della Corte, spesso citata sia nell'art. 8 che nell'art.6, riguardante il rispetto dei *civil rights*[40].

37" *Equipment Interference Code of Practice*, emesso in forza della Sezione 71 RIPA, ad integrazione del *Covert Surveillance and Property Interference Revised Code of Practice* del 2014, entrato in vigore in data 28 gennaio 2016, ma utilizzato in forma provvisoria sin dal 2015.

38 IPT/01/62 and IPT/01/77, Rulings of the Tribunal on preliminary issues of Law, 23 gennaio 2013, & 138 "The limits require a balance to be struck by the Secretary of State between basic common law rights and Convention rights of fair trial and open justice and the needs of national security and the public interest. In making the Rules the Secretary of State must ("shall") have particular regard to the two matters specified in section 69(6) (a) and (b). They obviously reflect the tension in Articles 6, 8 and 10 of the Convention between, on the one hand, the principles of fair trial and open justice normally applicable to the hearing and consideration of claims and complaints to a judicial body entrusted with the determination of civil rights and, on the other hand, the special needs and legitimate aim of preventing the disclosure of information prejudicial to national security and other aspects of the public interest". Tutte le decisioni del IPT sono accessibili attraverso il sito del tribunale, List of Judgments.

39" IPT/01/62 and IPT/01/77, citata.

40 IPT, citata, & 108: "In brief, viewing the concept of determination of "civil rights" in the round and in the light of the Strasbourg decisions, the Tribunal conclude that RIPA, which puts all interception, surveillance and similar .intelligence gathering powers on a statutory footing, confers, as part of that special framework, additional "civil rights" on persons affected by the unlawful exercise of those powers. It does so by establishing a single specialised

Tra i tanti aspetti di interesse, qui possono esserne citati solo alcuni, utili ai nostri fini. Il tribunale opera senza le limitazioni del processo *adversial* e può acquisire ogni genere di informazione, anche se non utilizzabile in una ordinaria Corte; per converso non ha poteri autoritativi sui testimoni. I convenuti (cioè i Servizi o le forze di polizia) possono adottare la politica di non confermare né smentire (NCND) quando una dichiarazione potrebbe mettere in pericolo il preminente interesse del segreto; la Corte ritiene questa politica compatibile con la giurisprudenza CEDU ritenendo che essa non escluda questo genere di cautele[41]. L'allontanamento dai principi del processo *adversial* è ampio, giunge fino alla possibilità di acquisizione di testimonianze e di documenti in segreto, senza successiva discovrey, neppure in sede di sommaria motivazione della decisione, ed è giustificato con le esigenze di tutela delle attività volte alla protezione degli interessi fondamentai dello Stato[42]. Il Tribunale può sedere anche in udienze non pubbliche e ciò non è ritenuto in contrasto con l'art.10 della CEDU.

Nel tempo il Tribunale ha seguito un approccio molto più aperto di quello che poteva apparire dalla fermezza della decisione procedurale, aprendo alla più ampia presenza delle parti e alla pubblicità. Va anche detto che l'impostazione indicata da questa decisione è stata ritenuta compatibile con i principi CEDU dalla sentenza Kennedy[43], che ha esaminato questioni attinenti all'applicazione degli artt. 6[44], 8 e 13 della Convenzione.

Nonostante questa regolamentazione, che può apparire ai nostri occhi molto poco compatibili con del controllo giurisdizionale, il IPT si è in realtà dimostrato un buon "cane da guardia" e ha dato ampia soddisfazione ai reclamanti, in casi che coinvolgevano la sicurezza nazionale in maniera molto significativa.

In realtà, più che attraverso l'aggiudicazione, spesso non in favore dei reclamanti, il risultato importante è stato ottenuto attraverso l'esercizio stesso della procedura, per la sua capacità conformativa delle attività

Tribunal for the judicial determination and redress of grievances arising from the unlawful use of investigatory powers".

41 IPT citata, & 111 "The procedural safeguards in respect of interference with Article 8 rights should be no less than those available under Article 6. Considerations of national security and public order serve as the basis of necessary and proportionate exceptions from the procedural rights normally available".

42 IPT, citata, & 174 ss.

43 Kennedy v. The United Kingdom *(Application no. 26839/05),* 18 May 2010

44 "…. the Court considers that the restrictions on the procedure before the IPT did not violate the applicant's right to a fair trial. In reaching this conclusion, the Court emphasises the breadth of access to the IPT enjoyed by those complaining about interception within the United Kingdom and the absence of any evidential burden to be overcome in order to lodge an application with the IPT. In order to ensure the efficacy of the secret surveillance regime, and bearing in mind the importance of such measures to the fight against terrorism and serious crime, the Court considers that the restrictions on the applicant's rights in the context of the proceedings before the IPT were both necessary and proportionate and did not impair the very essence of the applicant's Article 6 rights" (& 190). In particolare, la Corte ha ritenuto non in violazione dell'art. 6 la clausola, fondamentale per IPT, NCND, non confermato né negato.

controllate, come il tribunale stesso non manca di sottolineare[45]. Le richieste di fornire informazioni e documentazioni e la conseguente interlocuzione critica ha infatti portato a modifiche nei regolamenti e nelle prassi, in senso maggiormente garantista.

Ciò dimostra, ancora una volta, quanto sia importante più che la singola garanzia il reale contesto dei rapporti istituzionali, delle prassi, della concezione di sé che hanno i diversi attori, del ruolo che gioca la pubblica opinione.

Vediamone alcune applicazioni, oltre quelle già citate.

Il Tribunale è stato a volte investito della questione concernente i rapporti tra l'autorizzazione di acquisizione di dati sulla base del PACE (e quindi sulla base di un mandato dell'autorità giudiziaria) e quella emessa in forza del RIPA e dunque senza mandato ma con provvedimento del Segretario di Stato e delle altre autorità da questo delegate sulla base delle previsioni di legge.

Assai di recente il Tribunale ha esaminato la questione in un caso molto delicato, concernente un membro del parlamento e alcuni addetti alla vigilanza di Downing Street[46]. Caso delicato in quanto coinvolgente giornalisti e dunque profili attinente alla tutela della libertà di stampa. Su quest'ultimo aspetto[47], per la parte che qui rileva, il Tribunale ha statuito che la disciplina in vigore all'epoca dei fatti (2013) non era rispettosa della CEDU, in quanto consentiva l'acquisizione dei dati dei giornalisti senza controllo giurisdizionale.

45 Si è visto in Liberty e si vedrà tra breve in Privacy.

46 Decisione in data 17 dicembre 2015, IPT/14/176/H, News Group Newspapers Limited and Others v.v. The Commissioner of Police of the Metropolis.

47 Il Tribunale ha fatto applicazione dei principi della CEDU. Esso ha in primo luogo affermato in linea generale la legalità del provvedimento RIPA "Applying the principles set out by Lord Bingham in Gillan, and noting paragraph 77 of the judgment of the ECtHR in Gillan v United Kingdom [2010] 50 EHRR 1105, s 22 of RIPA does comply with the principle of legal certainty. The discretion granted to a designated person under s 22 is not unfettered. The law does "*indicate with sufficient clarity the scope of the discretion conferred on the designated person and the manner of its exercise*". S 22 requires that the exercise of the power be both necessary and proportionate. As Laws LJ noted in Miranda at paragraph 88 the discipline of the proportionality principle is one of the foremost safeguards. The decision of a designated person is subject to review by an independent Commissioner and, if a complaint is made, to a determination by this Tribunal. The power conferred by s 22 is subject to protection against arbitrary use.". Il Tribunale ha poi chiarito i termini entro i quali va accordata ai giornalisti una maggiore protezione: "In contrast to the powers under consideration in those cases, the power under s 22 does not enable the police to obtain access to journalistic material nor to intercept communications between a source and a journalist. The power is only to obtain communications data, which does not reveal the contents of any communication between the journalist and his source. Nor does the power require the journalist to take any step which would infringe the duty of confidence which he owes to the source, as the information is obtained directly from the CSP. As was stated in Goodwin at paragraph 40, limitations on the confidentiality of journalistic sources call for the most careful scrutiny. That careful scrutiny must start by recognising the limits of the power under s 22 and the fact that it neither permits the police to obtain journalistic material nor even, as was the case in Goodwin, imposes a legal requirement on a journalist to identify his source.". Va considerato che il PACE 2007 è stato emendato nel 2015, al fine di meglio tutelare la libertà di informazione.

Circa il rapporto tra RIPA e PACE, al di fuori del caso in cui è in discussione la particolare tutela accordata al giornalista e che richiede quindi il provvedimento giurisdizionale, il Tribunale ha ritenuto che le acquisizioni sarebbero state legittime in entrambe i casi e che non aveva dunque rilievo, ai fini della legalità della procedura, l'autorità da cui il provvedimento emanava. Anche il RIPA, infatti, impone uno scrutinio di sussistenza delle condizioni legittimanti l'acquisizione del dato, attraverso un provvedimento motivato e un circuito di verifica e controllo (non giurisdizionale)[48], nonché una valutazione di proporzionalità.

Il Tribunale distingue dunque nettamente tra la legalità della procedura seguita e la sussistenza dei requisiti in fatto[49] e la loro esposizione in motivazione.

In una recentissima decisione[50], il Tribunale è intervenuto nella materia delle CNE (*Computer Network Exploitation*), cioè nelle attività di hacking, comportante la raccolta massiva di dati, anche attraverso inoculazione di virus, e la loro conservazione.

Dopo una lunga e approfondita motivazione che merita un esame particolareggiato, che qui non può esser fatto, e sulla base di costanti richiami alla giurisprudenza della CEDU, il Tribunale conclude per la legittimità delle operazioni, ma distinguendo i diversi casi, prevedendo in ogni caso un'autorizzazione specifica, ponendo limiti e rilevando che l'asserzione della legittimità in generale di questo genere di provvedimenti e di azioni non esclude la violazione dei diritti dei singoli e il conseguente azionamento di rimedi.

In particolare, l'autorizzazione deve essere quanto più specifica possibile circa i dispositivi che devono essere oggetto dell'azione, anche se non necessariamente individuati con riferimento a singoli soggetti identificati, così da soddisfare i requisiti di legalità, necessità e proporzionalità.

48 "We are satisfied that s. 22 does contain a number of safeguards for the general run of criminal investigation cases. Those safeguards include those already noted at paragraph 97 above. The designated person, although not independent of the police force, is a senior officer, who is effectively required to exercise an independent judgment. The existence of oversight arrangements, including oversight by the Commissioner, is a strong factor in ensuring that the power under s 22 is properly exercised. The designated person knows that any decision to grant an authorisation, which is recorded in writing, may be subject to later review" (& 103).

49 "The main submission of the Respondent was that the Complainants' argument confuses the issue of proportionality with legality. The question is whether the police used the least intrusive measure, and that test focuses on the infringement of rights, not the means by which an order or authorisation is obtained. The intrusion is the obtaining of communications data which might reveal a journalist's source, not the making of an application to a designated person under RIPA or to a judge under PACE… omissis. .. We accept those submissions. It is clear from consideration of the cases of Roemen and Schmidt v Luxembourg Application No.51772/99 25 May 2003 (at paragraph 57) and Ernst v Belgium (2004) 39 EHRR 35 (at paragraph 103) that the issue on proportionality is directed to the effect of the infringement in question, not the procedure by which an authorisation or order is obtained. The communications data obtained, whether from a judge under PACE or from a designated person under s 22 of RIPA, is data which has the same effect of potentially revealing a journalist's source and thus the intrusion on rights is the same. It is that intrusion, not the procedure used to give it legal effect, which must be justified under the principle of proportionality." (& 90 / 91).

50" Giudizio reso il 12 febbraio 2016 nelle controversie riunite IPT 14/85/CH e IPT 14/120-126/CH, Privacy International e Grennet Limited e altri v. Secretary of State e GCHQ.

Il Tribunale conclude osservando che "l'utilizzo di CNE da parte di GCHQ, ora accertato, ha fatto sorgere ovviamente una quantità di serie questioni, che abbiamo cercato di risolvere al nostro meglio in questo giudizio. Chiaramente esso enfatizza la richiesta di un bilanciamento da stabilirsi tra le necessità impellenti delle Agenzie di Intelligence al fine di salvaguardare il pubblico e la protezione della riservatezza e della libertà di espressione del singolo. Siamo certi che con il nuovo *Codice Equipment Interference* e qualunque sarà la decisione del Parlamento sull' IP Bill (*Investigatory Powers Bill*) un corretto bilanciamento si viene realizzando nella materia oggetto della nostra decisione".

Queste ultime notazioni vanno lette alla luce della rivendicazione che a questo proposito il Tribunale aveva fatto del ruolo avuto dai suoi consulenti e dalle prospettazioni degli attori nel determinare la rivelazione delle regole poste a base delle attività segrete e della nuova disciplina, sollecitata anche dal Commissioner[51].

A dimostrazione dell'importanza della rete di controlli giudiziari, politici e più in generale attinenti al rispetto di prassi istituzionali, al di là delle singole aggiudicazioni.

51 "ii) There are now in the public domain what were previously "*below the waterline*" arrangements (see paragraph 7 in the Liberty/Privacy No.1 judgment) underlying both the Property Code and the E I Code, either redacted or gisted [sic!]. Whether or not in the event they are determinative in relation to the issues canvassed before us in relation to the question of accessibility or foreseeability under Articles 8 and 10 of the ECHR, it is valuable that they have been produced by the Respondents in these proceedings. This arose as a result of the disclosure sought by the Claimants, and by Counsel to the Tribunal, and requested by the Tribunal.
iii) Simultaneously with the preparation and eventual presentation of this case, there has been the consideration by David Anderson QC, the Independent Reviewer of terrorism legislation, in his Report dated June 2015, and subsequently the draft Investigatory Powers Bill ("the IP Bill") laid before Parliament in November 2015, which in its present form has been before us, both of which plainly drew upon the ideas and submissions which have now been openly canvassed before us" (& 11).