Politiche della sicurezza e diritti fondamentali*

di *Armando Spataro*

Prima parte

Il cosiddetto "terrorismo islamico" e la centralità della giurisdizione. Il sistema italiano: dagli "anni di piombo" al rifiuto della "war on terror". Le leggi post stragi di New York (2001), Londra (2005), Parigi (2015)

1. Premessa e rilievi critici ad altri interventi

Il mio intervento sarà ovviamente il frutto della mia esperienza di pubblico ministero, in particolare di quella maturata, praticamente sin dal mio ingresso in magistratura e con poche ma brevi interruzioni, nel settore delle indagini sul terrorismo interno e internazionale.

In particolare tratterò il tema, forse ancora non sufficientemente esplorato, della effettiva utilità ai fini di tali indagini delle raccolte di dati e informazioni sulle persone,

---

* L'intervento di A. Spataro ha come tema centrale la legittimità ed efficacia delle raccolte dei dati personali rispetto alle indagini penali riguardanti il terrorismo internazionale, nonché rilievi critici sugli indirizzi che sembrano prevalere nella politica antiterrorismo dell'Unione Europea. La relazione coincide, a partire dal par. 2, con quella dal titolo "*Quanto controllo può sopportare un democrazia?",* tenuta a Roma, il 28 maggio 2016, nell'ambito del Convegno organizzato dal Garante per la protezione dei dati personali sul tema *I nuovi confini della libertà – La società sorvegliata.* Vi sono contenute citazioni, anche con aggiornamenti, da precedenti relazioni ed articoli, tra cui *Otto anni dopo l'11 settembre.- Il modello anglosassone e quello europeo nell'azione di contrasto del terrorismo internazionale, Questione Giustizia", n. 5/2009* (Franco Angeli Ed.)

che la moderna tecnologia ci consente, nonché sull'errata impostazione, che sembra cara all'Europa, di voler privilegiare l'attività della cd. *intelligence* nel contrasto del terrorismo, trascurando il tema della cooperazione giudiziaria.

Vorrei premettere, però, anche alla luce del contenuto di altri interventi, alcune osservazioni sulle motivazioni e definizioni del tragico terrorismo dinanzi al quale ci troviamo, nonché sulla necessità di non trascurare, ed – anzi – di valorizzare affinandole, le tecniche investigative che abbiamo in passato adottato contro il terrorismo interno.

Condivido, in particolare, gran parte dell'intervento di Giovanni Salvi, ma alcune sue valutazioni mi lasciano perplesso.

Parto dalle motivazioni del terrorismo internazionale. In questo sono d'accordo con il Procuratore generale di Roma: si tratta, pur con le precisazioni che seguono, di motivazioni in generale religiose (non dunque politiche in senso stretto, né economiche, né di liberazione di territori "occupati"), come ho avuto modo di affermare sin dal 2008 in miei precedenti interventi[1].

Ma partendo da queste premesse (sulle quali mi si perdonerà la sintesi), Giovanni Salvi giunge a respingere la definizione di «terrorismo cosiddetto islamico» che altri suggeriscono di utilizzare in quanto *"politically correct"*. Io, invece, la ritengo del tutto corretta e non certo in ossequio a logiche di mediazione che non mi hanno mai appassionato. Avverto anche la necessità di precisare quanto sia fuorviante affermare che *«l'attuale terrorismo non può essere definito "così detto islamico", non più di quanto le Brigate Rosse potessero esser dette "sedicenti"»*. L'esempio non è pertinente: negli "anni di piombo" l'errore era politico e spesso strumentalmente voluto; oggi abbiamo invece il dovere di rispettare le religioni diverse dalla nostra e di non generalizzare.

Se sono convinto assertore della necessità di adottare la definizione di «terrorismo cosiddetto islamico» (anziché quella di «terrorismo islamico»), ciò dipende anche dalla mia personale esperienza di investigazione (che mi ha portato a conoscere

1 Gli interventi cui si fa riferimento sono: 1) *Perché si diventa terroristi? Le esperienze di un Procuratore*, in *Journal of International Criminal Justice* (Oxford Journals - Oxford University Press - Aprile 2008); 2) *Cosa induce tante persone ad abbracciare il terrorismo? Perché si diventa terroristi? Le esperienze di un Pubblico ministero,* in *Voci contro la barbarie - La battaglia per i diritti umani attraverso i suoi protagonisti,* a cura di Antonio Cassese, Feltrinelli (novembre 2008); 3) *Colloquio sul terrorismo internazionale* con Diomira Petrelli, in *Rivista di Psicoanalisi* n. 3.2008 della Società Psicoanalitica Italiana, numero dedicato a *Terrore e Non pensiero*.

intercettazioni, documenti, dichiarazioni di collaboratori maghrebini) e di studio: ho fatto parte, ad esempio, di un gruppo di studio della N.Y University che ha operato per vari anni, nel decennio scorso, per intensificare la conoscenza di questo terrorismo e le possibili forme di effettiva collaborazione internazionale. Ebbene, non potrò dimenticare le richieste rivolte a noi europei da autorevoli esponenti delle magistrature, delle forze di polizia e da accademici di vari Paesi islamici da me incontrati in quelle periodiche occasioni di chiamare questo terrorismo «*so-called islamic terrorism*», unica espressione idonea – ci dicevano – a evitare ogni impropria, se non offensiva, generalizzazione che potrebbe derivare anche dall'uso di definizioni molto diffuse come «terrorismo jihadista» o «fondamentalista». Il «Jihad», ad esempio, è un termine spesso erroneamente considerato equivalente, in Occidente, a «guerra santa». Ma, tra le tante possibilità, la più corretta è altra: esso significa letteralmente «lotta», «sforzo» compiuto «sulla via di Dio» in nome dei principi in cui crede, ma non con armi, bombe e stragi, pur se, nella convinzione dei gruppi terroristici, assume la valenza di obbligo, che ricade sulla intera comunità, di lotta con metodi violenti per l'affermazione della religione islamica. Il tutto in una distorta visione religiosa del mondo che, fondata sulla sua divisione in fedeli ed infedeli e reiterata in ogni forma di indottrinamento, conduce alla deumanizzazione dei potenziali obiettivi, alla intolleranza del dubbio o del dissenso, alla adorazione dei *lead*er di turno, alla disponibilità a distruggere storia e cultura degli infedeli ed a sovvertire contemporaneamente i regimi corrotti ed apostati dello stesso mondo musulmano. Ed a sua volta, anche il termine «fondamentalismo» non può essere confuso con la posizione di chi predica la violenza per l'affermazione della religione islamica.

Si tratta di conclusioni cui si può agevolmente pervenire, nell'ottica e sulla base dell'esperienza dell'investigatore, grazie alle dichiarazioni rese dai collaboratori processuali che in Italia, anche in questo campo, si sono manifestati e all'analisi del contenuto di documenti ideologici diffusi a livello internazionale tramite il web o sequestrati nel corso di varie indagini: univocamente essi dimostrano che la distorta prospettiva propria dei terroristi costituisce la ragione principale dei loro comportamenti, mentre non riveste praticamente alcun rilievo la mera aspirazione a liberare specifici territori occupati e popoli oppressi. Le varie "guerriglie" o "guerre", di volta in volta in atto o imminenti, anzi, costituiscono mere occasioni – per quanto importanti – per attuare un programma di lotta che è assai più vasto e che, nel dare concreto significato alla parola Jihad, si propone l'obiettivo di riportare la legge islamica "pura" e il Califfato agli stessi confini della sua massima espansione storica, comprese parti delle terre spagnole e dei Balcani. Non penso che i *leaders* di IS credano

davvero che questo obiettivo sia raggiungibile, ma intanto lo diffondono: e questo paga in termini di attrazione!

In questa cornice che racchiude attività e programmi di tutti i gruppi, di diverso e nuovo – rispetto alle modalità di azione di quelli oggetto delle inchieste dello scorso decennio – vi è solo la sopravvenuta capacità di sfruttare la modernità e le potenzialità del web ai fini della propaganda, dell'arruolamento e persino dell'addestramento. È una capacità, ripeto, anche di attrazione, che è emersa e si è sviluppata negli ultimi due-tre anni, soprattutto ad opera dell'IS (prima denominato ISIS o ISIL)[2] che ha così visto crescere le proprie milizie e le possibilità di impegno nei territori di guerra.

Sul tema della definizione di questo terrorismo, si veda anche *Perché è giusto non chiamare "islamico" il terrore dell'IS*, di Fareed Zakaria (La Repubblica, 21.2.2015), a commento di analoga posizione espressa niente meno che dal presidente degli Stati Uniti B.Obama in una pubblica conferenza.

Orbene, io mi sento più vicino alla posizione espressa dal presidente Obama che a quelle di chi – non me ne vorrà il collega – pensa il contrario, arrivando a ritenere che la scelta del velo non sia mai libera per la donna islamica: mi auguro che anche su aspetti come questi si possa pervenire ad una omogeneità di visione circa la pienezza dei diritti delle persone, ma rivendico di avere – come pubblico ministero – chiesto ed ottenuto dal Tribunale di Milano che una donna islamica, dopo la identificazione a volto scoperto in una stanza separata, da parte di una cancelliera, fosse sentita come testimone, in aula, con il volto coperto, come da lei richiesto per motivi religiosi.

Tanto premesso, sono ovviamente d'accordo con Giovanni Salvi sulla necessità di aggiornare le nostre conoscenze rispetto non solo agli "anni di piombo" (che pure

2 Lo Stato Islamico (abbreviato IS) è il gruppo terrorista islamista attivo in Siria e Iraq, il cui attuale capo, Abu Bakr al-Baghdadi, nel giugno 2014 ha unilateralmente proclamato la nascita di un Califfato nei territori caduti sotto il suo controllo. Prima della proclamazione del Califfato, si faceva chiamare Stato Islamico dell'Iraq e al-Sham (comunemente tradotto come Stato Islamico dell'Iraq e della Siria: abbreviato ISIS) o Stato islamico dell'Iraq e del Levante (abbreviato ISIL). L'avere tolto dai precedenti acronimi le due ultime lettere è ritenuto da Renzo Guolo (*Così il popolo della jihad cresce nelle nostre città,* La Repubblica, 24 marzo 2016) il *«capolavoro di Abu Bakr al-Baghdadi che è riuscito a dar vita allo "Stato islamico", non più localizzato in Siria ed in Iraq, ma con ambizioni e proiezioni universali: coronate nell'autoproclamazione e nella rifondazione del Califfato. Mossa che nemmeno Osama Bin Laden all'apogeo della sua potenza aveva osato»*.

hanno partorito la spontanea attitudine della nostra magistratura al coordinamento investigativo ed al virtuoso rapporto di confronto e direzione rispetto alla polizia giudiziaria: patrimonio da diffondere anche fuori dall'Italia), ma anche – aggiungo – rispetto alla evoluzione del terrorismo internazionale che è cambiato sin dai primi anni di questo decennio.

Sono utili in proposito anche le recenti valutazioni e ricostruzioni di Bruno Megale, uno dei più esperti investigatori di cui disponiamo[3] secondo cui :

«se da un lato, in Occidente, il biennio 2008/2010 ha fatto registrare un sostanziale arretramento dell'operatività delle organizzazioni terroristiche, duramente colpite dall'attività repressiva anche a livello militare (fino all'uccisione di Osama Bin Laden nel maggio 2010), si è assistito dall'altro al proliferare di episodi criminali frutto di *spontaneismo operativo* svincolato da contesti organizzativi.

Gli eventi politici connessi alle cd "primavere arabe", che a partire dal 2010 fino al 2012 hanno interessato tutti i Paesi del *Maghreb* e mediorientali, hanno generato l'illusione di un *risveglio democratico nel Mondo musulmano,* suscitando il plauso delle democrazie occidentali che hanno sostenuto questo processo di rinnovamento (la rivoluzione di Facebook) nella convinzione che i *germi* della democrazia innescassero irreversibili cambiamenti in tutta l'area. Ma le sommosse nei Paesi musulmani, dopo una prima fase di entusiasmo generalizzato, hanno ampiamente disatteso le aspettative. Nella realtà la rivolta popolare, propagatasi rapidamente in tutta la regione anche per il peggiorare delle condizioni sociali dovute alla crisi economica, se da un lato ha avuto gioco facile nel collasso dei Governi tacciati di nepotismo e corruzione, dall'altro non ha trovato una efficace sponda nel mondo laico per la mancanza di partiti o formazioni in grado di trasformare le istanze *rivoluzionarie* in un nuovo progetto politico. Ciò ha determinato nel tempo l'affermazione in tutti i Paesi dei movimenti islamisti, gli unici capaci di intercettare il consenso delle masse in virtù della loro organizzazione e del radicamento sul territorio, nonché della capacità di attendere ai bisogni primari della popolazione attraverso il sostegno delle moschee.

Oggi l'illusione occidentale è naufragata di fronte all'affermazione dello Stato Islamico, che ha saputo convogliare tutte le risorse islamiste sul terreno con migliaia di

3 Le parole qui riportate sono tratte da un relazione tenuta nel gennaio del 2016 del dr. Bruno Megale, già dirigente della Digos della Questura di Milano ed ora Questore a Caltanissetta, presso la Scuola superiore della magistratura di Scandicci (FI).

combattenti provenienti dai campi tunisini e libici, ma anche volontari dall'Europa e dal Nord America. Un rigurgito islamista che ha prodotto i suoi effetti anche in Europa e negli Stati Uniti con azioni di terrorismo ascrivibili a lupi solitari, alimentati da una miscela di pensiero islamico/radicale e risentimento antioccidentale.

Il 29 giugno 2014 Abu Bakr al Baghdadi ha proclamato la nascita del Califfato (K*hilafah*) nei territori dello *Sham*, compresi tra Siria ed Iraq sunnita, che ha assunto la denominazione di Stato Islamico. Il Califfato nella tradizione islamica incarna infatti la società perfetta del Profeta Muhammad e dei primi quattro Califfi (i *rashiduna* - ben guidati), e racchiude in sé l'idea originaria dell'unicità del mondo musulmano (*Ummah*) sotto la guida di una figura autorevole che abbia il consenso di tutta la comunità.

L'autoproclamato Califfo pur non ottenendo alcun riconoscimento formale da parte delle più eminenti figure teologiche del mondo islamico, con il suo gesto di rottura ha prodotto un effetto emulativo delle altre componenti radicali, che si sono affrettate a riconoscerne la *leadership* con un giuramento di fedeltà (*bayat*).

La "proposta politica" di *Abu Bakr al Baghdadi* é stata il detonatore per un rinnovato attivismo di tutti gruppi *jihadisti* operativi nei teatri africano e mediorientale.

Ansar Al Shariah libica, sotto l'impulso dell'IS, ha dato vita ad un "califfato" nella provincia di Derna poi a Sirte, sottratte al controllo delle autorità centrali; in Somalia i combattenti di *alShabaab* hanno intensificato le operazioni terroristiche nel vicino Kenya; in Nigeria i miliziani di *Boko Haram,* hanno proclamato la nascita di un "Califfato" nel nord del Paese, accentuando il conflitto interconfessionale con azioni stragiste e sequestri di giovani donne nei villaggi a maggioranza cristiana.

Insomma, è cambiato lo scenario internazionale: sotto l'aspetto politico/amministrativo, il Califfato ha imposto un controllo minuzioso su una vasta porzione di territorio tra Siria e Iraq, che amministra in autonomia secondo i dettami della legge islamica, attingendo dal territorio stesso le risorse, anche finanziarie, necessarie alla sua sopravvivenza (sfruttamento delle risorse petrolifere e derivati, pagamento dei tributi etc..); nella capitale Raqqa insistono le più importanti istituzioni, la sede del Governo centrale nel Municipio della città, il Tribunale della Shaaria, il Quartier generale delle operazioni militari. Sotto l'aspetto sociale, infine, l'Is nei territori sotto il suo controllo ha avviato un efficace sistema sanitario, un programma scolastico articolato su 12 classi, un corpo di polizia islamica, anche stradale, per la verifica del rispetto dei precetti shariatici, una polizia di sicurezza ed accesso al Paese con *check-point* di controllo, un puntuale sistema di riscossione tributi e pagamento dei

compensi dei combattenti e dei dipendenti pubblici, oltre ad un sussidio economico per le famiglie con più figli.

L'organizzazione del Califfo *al-Baghdadi*, peraltro, ha una visione *apocalittica* del proprio ruolo e si pone come ultimo argine alla cultura occidentale e alle "devianze" dello stesso mondo islamico, in primo luogo gli sciiti.

Questa logica è sottesa nei video di propaganda diffusi in rete dai militanti dell'Is, in cui sono documentate le atrocità verso i nemici e le spietate esecuzioni dei prigionieri, siano essi soldati iracheni, siriani fedeli al regime, oppure ostaggi occidentali.

Una propaganda che si avvale di meccanismi comunicativi di *immediatezza* ed *ipermediazione* – ovvero la moderna moltiplicazione ed interazione dei media – per raggiungere il maggior numero di destinatari e fare *audience*.

Se tutto è cambiato, è evidente che non si possono semplificare l'analisi e le definizioni del cd. terrorismo islamico, ignorandone evoluzione, nonché guerre civili, divisioni e persecuzioni anche all'interno del mondo islamico. È impossibile ricondurre ad unità o catalogare le varie forme di manifestazione del terrorismo nel mondo: persino la minoranza musulmana ne è vittima nel nord del Myanmar. La confusione regna sovrana anche sulle forme di finanziamento del terrorismo dell'IS: si parla di fonti costituite da traffico di esseri umani e di stupefacenti, ma ancora non sappiamo esattamente dove e quando ciò risulti effettivamente avvenuto. E persino le opzioni belliche nei territori occupati dall'IS, a prescindere da ogni altra considerazione e dal fatto che rientrano nelle competenze politiche, sono rese ancor più difficili dalla impossibilità di distinguere amici da nemici, categorie a loro volta cangianti. Lo affermano anche esperti vertici delle strutture militari.

Occorrono allora, «*per evitare di suicidarci in questo scontro di lungo periodo … freddezza, pazienza, capacità di assorbire attacchi e provocazioni*[4]» a partire dalla necessità di non definire questo terrorismo "islamico" *tout court*, poiché, come ancora ricorda Lucio Caracciolo, «*in questo universo paranoico, l'umanità è spartita in cinque famiglie. Dal Bene al Male, dal puro all'impuro: noi giusti, i "cattivi musulmani (sunniti deviati); gli eretici (sciiti e seguaci di altre correnti eretiche); gli ebrei; i crociati, ovvero gli occidentali identificati con un cristianesimo aggressivo*»[5].

4 L. Caracciolo, *Scacco al terrore in quattro mosse*, *La Repubblica*, 17 novembre 2015.

5 L. Caracciolo, *La strategia della paura*, *La Repubblica*, 1 dicembre 2015.

Finisco i miei rilievi critici ad altri interventi, dicendo che quando si invocano altre vie per il contrasto a questo terrorismo, esse andrebbero meglio specificate. Siamo d'accordo sulla grande importanza delle informazioni raccolte anche in zone di conflitto, ma non sono chiare alcune affermazioni come quelle secondo cui ciò renderebbe «necessario riflettere su come assicurare agli interlocutori la segretezza ... delle metodologie utilizzate, realizzando un bilanciamento tra questa esigenza e quella repressiva», o sul rilievo da attribuire – come in altri Stati europei – «alla raccolta di informazioni al di fuori del diretto controllo giudiziario» o, ancora, sulla necessità di «meglio tarare i rapporti tra repressione e raccolta di dati provenienti dalla *intelligence*». Insomma, io credo che – come le pagine che seguono spero dimostreranno – sia piuttosto necessario sforzarsi di diffondere le regole efficienti e rispettose dei diritti individuali che il nostro sistema già prevede, piuttosto che "tararle" sulle aspettative e sulle non condivisibili visioni della lotta al terrorismo proprie di altri Governi, per di più non solo visibilmente inefficaci, ma spesso contrastanti con i principi affermati dalla Corte europea dei diritti dell'uomo. Il che non è certo un mantra inutile e non rischia affatto – come sostiene Massimo Donini – di trasformare la magistratura «in strumento di lotta perdendo il suo carattere di imparzialità a garanzia di tutti». Del suo equilibrio e della sua terzietà, infatti, la magistratura italiana ha già dato ampia prova.

2. Brevi cenni al passato

Ritengo, a questo punto, di dover fare brevissimi cenni al passato: spesso ricordare è necessario ed utile per il presente e per il futuro. In questo caso aiuta a pervenire ad una conclusione che anticipo: le conoscenze dei fenomeni criminali su cui si indaga e le tecniche di accertamento di fatti e responsabilità personali devono essere aggiornate, ma non possono determinare una benché minima lesione del sistema dei diritti individuali il cui rispetto ha caratterizzato l'azione delle nostre istituzioni contro il terrorismo interno, contro la mafia ed altri gravi fenomeni criminali.

Voglio dire, allora, che gli anni di piombo hanno visto la capacità delle nostre istituzioni di affrontare razionalmente e correttamente il terrorismo interno fino a sconfiggerlo alla fine degli anni ottanta. Uso la parola "sconfiggere" anche se allude ad una battaglia o ad una guerra, cioè ad una visione di quegli anni che non mi piace affatto: non vi fu guerra, se non quella unilateralmente dichiarata da ottusi criminali. Siamo stati capaci di vincere quel terrorismo nell'assoluto rispetto delle regole e dei diritti delle persone, anche di quelli dei responsabili di gravissimi reati.

La sintesi del mio pensiero (condiviso da molti giuristi, a partire dal compianto prof. Vittorio Grevi) sta in quella famosa frase – che cito spesso anche quando racconto quegli anni nelle scuole – del presidente Pertini, che disse: *«Abbiamo sconfitto il terrorismo nelle aule di giustizia e non negli stadi»*.

Un'affermazione che allude alla correttezza dell'azione istituzionale ed alla centralità dell'azione giudiziaria: la magistratura italiana, infatti, può rivendicare di avere rivestito, insieme alla polizia giudiziaria, un ruolo decisivo nel contrasto del terrorismo interno (quello, appunto, dei cosiddetti *"anni di piombo"*).

Proprio negli anni più bui di quel terrorismo, cioè negli anni '70 e durante buona parte degli anni '80, la magistratura fu capace di esprimere un eccellente livello di professionalità: specializzazione, lavoro di gruppo, coordinamento spontaneo tra uffici giudiziari, scambio immediato delle notizie, raccordo effettivo e virtuoso con la polizia giudiziaria, capacità di gestione di un fenomeno divenuto quasi di massa come quello dei "*pentiti*" e rispetto delle garanzie degli imputati furono i fattori che ne caratterizzarono l'azione.

Una correttezza che si manifestò anche nella interpretazione ed applicazione di una legislazione che qualche commentatore, non sempre in buona fede, continua a definire "emergenziale" . Si allude, con tale definizione, a presunti strappi al sistema dei diritti da cui quella legislazione sarebbe stata caratterizzata trascurando il fatto che fu, invece, utile nella individuazione di strumenti adeguati per la sconfitta del terrorismo interno e che proprio magistrati e forze di polizia seppero disinnescarne alcune criticità .

Va anche doverosamente sottolineato che pubblici ministeri e giudici istruttori, in quegli anni, non intrattennero – salvo che in un caso riguardante lo stragismo di destra, da cui scaturirono polemiche ed un processo penale – rapporti funzionali con i Servizi d'informazione ma solo con la polizia giudiziaria: non certo per preconcetta ed ingiustificata diffidenza nei confronti dei primi, ma per la precisa consapevolezza della diversità di ruoli e competenze tra polizia giudiziaria e Servizi stessi. Non a caso per i Servizi, riformati nel '77, fu previsto l'obbligo di riferire le notizie di reato alla polizia giudiziaria, tramite i rispettivi vertici: un obbligo che permane con la riforma del 2007[6] e che consente di evitare sovrapposizioni di interventi forieri di equivoci ed errori.

6 Il tema delle diverse competenze di Pg e Servizi d'informazione verrà comunque trattato più avanti, anche con riferimento all'attualità.

Ed infine non si manifestò affatto la singolare ed anomala tendenza di alcuni procuratori generali ad assumere alcune improprie funzioni di coordinamento investigativo che si va attualmente manifestando rispetto al terrorismo internazionale.

3. Il rifiuto della teoria della *War on Terror*

Saltando in avanti, in particolare alla fine degli anni novanta ed alla progressiva "esplosione" del terrorismo internazionale, o del cosiddetto terrorismo islamico, abbiamo saputo dire "no!" alla teoria statunitense della Wot (*War on* Terror) o guerra al terrorismo, che non solo comporta la pratica delle *extraordinary renditions*, delle connesse torture e la creazione del cosiddetto "sistema Guantanamo", ma che ha determinato deviazioni dallo Stato di diritto che giudico inaccettabili e che tali sono state recentemente ritenute anche dal Senato americano[7]. E tali deviazioni si sono manifestate anche in Paesi a noi vicini, quasi come reazioni "istintive" al terrorismo, nel solco delle scelte statunitensi proprie dei *Patriot Acts* (il noto pacchetto composto da vari provvedimenti tra leggi *tout court* e *Presidential Orders*). Di qui il rafforzamento delle competenze tipicamente proprie degli apparati di polizia e di *intelligence*, che, a titolo di esempio, ha portato all'introduzione, in Gran Bretagna, del fermo dei sospetti terroristi per ben ventotto giorni (ma l'allora premier inglese Gordon Brown avrebbe preferito un termine di quarantadue giorni) o dell'uso esteso dei *control orders* (fortunatamente oggetto di una decisione unanime di nove giudici della House of Lords del giugno 2009 che li ha praticamente cancellati), vale a dire provvedimenti amministrativi contenenti pesanti restrizioni della libertà (sorveglianza elettronica, limite orario di rientro nell'abitazione privata, divieto di incontro con determinate persone e di frequentazione di determinati luoghi, divieto di usare il telefono e di guidare, preghiere in moschee ecc.) adottati nei confronti di persone sospettate di attività terroristiche, che non potevano essere legalmente processate a causa della segretezza imposta sulle fonti di prova o di sospetto a loro carico. In Francia esiste ancora la *garde à vue,* che consente alla polizia

7 Il 9 dicembre del 2014, il Senato Usa ha diffuso un rapporto di circa 500 pagine ("rapporto Feinstein" dal nome della presidente della Commissione sull'*intelligence* del Senato, la democratica californiana Dianne Feinstein), fondato anche sulle ammissioni di molti dirigenti della Cia, rendendo ufficialmente note le torture di ogni tipo (*water-boarding* incluso*)* e la prassi delle *extraordinary renditions*, attuate dalla stessa Cia per circa un decennio nel quadro di una inaccettabile strategia di lotta al terrorismo internazionale, proprio in quella sede giudicata inutile rispetto al dichiarato obiettivo di contrasto del terrorismo internazionale.

di detenere e interrogare i fermati per terrorismo per quattro giorni, in assenza di intervento di magistrati e di avvocati, ciononostante ottenendo dichiarazioni costituenti prove valide nei processi. L'affievolirsi dei controlli giurisdizionali è diventata persino eclatante nelle norme in materia di espulsioni degli stranieri per motivi di prevenzione del terrorismo che si diffondono in ogni parte d'Europa.

Anche a tutto questo, e ad altro ancora, l'Italia ha saputo dire di "no", nonostante l'approvazione di leggi specificatamente destinate a contrastare questo fenomeno sia intervenuta all'indomani di tragedie vere e proprie

4. La normativa italiana in tema di terrorismo internazionale: cenni

La specifica normativa in tema di terrorismo internazionale ha riguardato i settori del diritto penale, della procedura penale, della esecuzione delle pene, delle misure di sicurezza, della attività di prevenzione, delle espulsioni degli stranieri, della organizzazione della magistratura e delle forze di polizia, del coordinamento investigativo, della raccolta di dati personali, nonché la disciplina amministrativa di una serie di attività ritenute degne di attenzione a fini di prevenzione di rischi di attentati. E le direttive internazionali in materia di terrorismo sono state recepite in Italia – pur se con molti vuoti – attraverso gli interventi normativi più importanti, cioè quelli intervenuti dopo l'11.9.01 e dopo gli attentati di Londra del luglio del 2005.

Questo, comunque, l'elenco di tali interventi:

- i tre Decreti Legge emanati dopo l'11 settembre 2001[8], tra cui il più importante è

8 Questi, più in dettaglio, i provvedimenti cui ci si intende riferire:

- Decreto legge 28.9.2001 n. 353, convertito nella legge 27.11.2001 n. 415 recante «*Disposizioni sanzionatorie per le violazioni delle misure adottate nei confronti del regime dei Talebani*»;
- Decreto legge 12.10.2001 n. 369, convertito nella legge 14.12.2001 n. 431 recante «*Disposizioni urgenti per contrastare il finanziamento del terrorismo internazionale*», che ha introdotto il Comitato di sicurezza finanziaria, costituito presso il ministero dell'Economia e delle Finanze e disciplinato la procedura di congelamento dei beni di persone ed associazioni sospette;
- Decreto legge 18.10.2001 n. 374, convertito nella legge 15.12.2001 n. 438 recante «*Disposizioni urgenti per contrastare il terrorismo internazionale*», che ha costituito l'intervento normativo più rilevante e che, tra l'altro, ha introdotto (al di là di quanto si dirà appresso):

sicuramente il dl 18.10.2001 n. 374, convertito nella legge 15.12.2001 n. 438 che, con modifiche del codice penale e del codice di procedura penale, ha rimodulato le norme già esistenti per fronteggiare il terrorismo interno, in particolare introducendo il reato di «*associazione con finalità di terrorismo internazionale*» (art. 270-*bis* cp), e prevedendo, sul versante procedurale, la competenza distrettuale per i reati con finalità di terrorismo, nonché altre innovazioni atte a rinforzare le possibilità investigative.

Tra queste vanno citate, in relazione al tema qui in discussione (tecnologie e strumenti per raccolta dati a fine investigativo), le seguenti possibilità che verranno appresso illustrate:

a) quella di effettuare intercettazioni in via preventiva, su autorizzazione del pm, i cui esiti, come è noto, non possono avere valenza probatoria e processuale;

b) quella di effettuare operazioni sotto copertura.

- il dl 27 luglio 2005, n. 144, conv. con modificazioni nella l 31 luglio 2005, n. 155 (cd. decreto Pisanu), successivo all'attentato di Madrid dell'11 marzo 2004 e, soprattutto, a quello londinese del 7 luglio 2005, che – tra l'altro – ha previsto una migliore definizione della «*condotta con finalità di terrorismo*» (art. 270-*sexies* cp: tali condotte sono state tipizzate attraverso formule che si ispirano alla nozione di terrorismo internazionale ed alla formulazione adottata dall'art. 1 della

---

- il reato di «*Associazione con finalità di terrorismo anche internazionale*» (nuova formulazione dell'articolo 270 *bis* del Codice penale);
- la possibilità, in analogia con quanto previsto nel settore dell'"antimafia", di effettuare intercettazioni telefoniche, ambientali e di flussi informatici in presenza di *sufficienti* indizi di reato e di *necessità* delle intercettazioni (mentre il regime ordinario prevede la presenza necessaria di *gravi* indizi e di *assoluta indispensabilità* delle intercettazioni);
- in analogia con quanto previsto per il contrasto della mafia, la competenza delle 26 Procure della Repubblica presso le sedi di distretto (e non più delle 166 costituite presso ogni Tribunale) a condurre le indagini in materia di terrorismo, al fine di garantire maggiore specializzazione e concentrazione del sapere investigativo;
- l'estensione al settore del terrorismo internazionale delle misure di prevenzione personali e reali, originariamente previste per contro la mafia.

Decisione Quadro del Consiglio dell'Unione europea del 13 giugno 2002)[9].

Anche in questo caso, in relazione al tema oggetto di questo intervento, vanno menzionate alcune scelte rilevanti:

a) la possibilità per i direttori dei Servizi di informazione, sul presupposto di una delega politica, di richiedere di essere autorizzati dalle Procure generali presso le Corti d'appello allo svolgimento di intercettazioni preventive[10];

---

9 Il Decreto-legge 27.7.2005 n. 144 recante misure urgenti per il contrasto del terrorismo internazionale, convertito con legge 31 luglio 2005 n. 155, ha pure.introdotto:

a) il «permesso di soggiorno a fini investigativi» (art. 2 del dl) che nasce dalla logica premiale che già da tempo l'ordinamento italiano prevede nei confronti dei collaboratori processuali in tema di criminalità mafiosa e terroristica (oltre che in vari altri settori criminali);
b) un complesso di nuove misure specificatamente atte alla prevenzione del rischio di attentati contro l'incolumità pubblica, attraverso l'introduzione di più rigorose regolamentazioni amministrative di attività astrattamente pericolose (in tale direzione vanno le nuove norme integranti la disciplina amministrativa degli esercizi pubblici di telefonia e *internet* di cui all'art. 7, delle attività concernenti gli esplosivi di cui all'art. 8, dell'attività di volo di cui all'art. 9, della prevenzione antiterroristica negli aeroporti di cui all'art. 9 *bis* e dei servizi di vigilanza che non richiedono l'impiego di personale delle forze di polizia di cui all'art.18);
c) nuove norme in materia di espulsioni degli stranieri per motivi di prevenzione del terrorismo;
d) la nuova figura di reato di «possesso e fabbricazione di documenti di identificazione falsi», validi per l'espatrio, con conseguente ampliamento delle ipotesi di arresto obbligatorio e facoltativo in flagranza di reato, nonché di fermo di indiziati di delitto (artt. 10 e 13);
e) la estensione da 12 a 24 ore del cd. fermo per identificazione personale**,** che risponde ad una obiettiva e frequente difficoltà nell'accertamento rapido della reale identità delle persone (specie se provenienti da Paesi extracomunitari) e della genuinità dei loro documenti personali;
f) nuove previsioni di reati nel Codice penale (l'arruolamento con finalità di terrorismo anche internazionale – *ex* art. 270 *quater* cp – e.l'addestramento ad attività con finalità di terrorismo anche internazionale – *ex* art. 270 *quinquies* cp – che prevede la punizione anche della persona addestrata) e la migliore definizione giuridica dei reati di terrorismo (sono state tipizzate – *ex* art. 270 *sexies* – le «condotte con finalità di terrorismo», attraverso formule che si ispirano alla nozione di terrorismo internazionale ed alla formulazione adottata dall'art. 1 della Decisione Quadro del Consiglio dell'Unione europea del 13 giugno 2002).

10 Tale potere autorizzativo, come si dirà appresso, è stato poi attribuito al solo Procuratore generale presso la Corte d'Appello di Roma.

b) l'obbligo di identificazione degli acquirenti di schede elettroniche (Sim) per telefonia mobile, di conservazione dei dati del traffico telefonico e telematico ed il nuovo regime di acquisizione dei dati stessi ai fini processuali di cui si parlerà appresso, comunque previsto sulla base di provvedimenti autorizzativi dell'Autorità giudiziaria.

c) il dl 18 febbraio 2015, n. 7, conv. con modificazioni nella l. 17 aprile 2015, n. 43, successivo alla strage parigina del 7 gennaio 2015 nella sede del periodico Charlie Hebdo, con cui finalmente è stata istituita la Direzione nazionale antiterrorismo all'interno della già esistente struttura di quella antimafia, così realizzando l'auspicio formulato da circa 25 anni dai magistrati italiani che si sono occupati di terrorismo, nonché dal Csm sin dal 2006. Sono stati dunque estesi al settore del terrorismo poteri e competenze del preesistente Procuratore nazionale antimafia[11].

Con l'intervento normativo del 18 febbraio 2015, sempre per la parte che interessa il tema qui in discussione:

a) è intervenuta una stretta sulla propaganda via web, strumento chiave dell'Is e di altre formazioni terroristiche. Di qui un pacchetto di previsioni mirate, tra cui quella che impone ai *providers*, su richiesta dell'Autorità giudiziaria procedente, di inibire l'accesso ai siti utilizzati per la propaganda terroristica o, su decreto motivato del pm ed in presenza delle condizioni di legge (vedi appresso),

---

11 Non appare necessaria, in questa sede, l'illustrazione dettagliata del contenuto del dl in questione che, comunque, ha anche introdotto o modificato varie norme penali e procedurali, nonché modifiche in materia di misure di prevenzione personali e di espulsione, nella parte relativa alle «*Misure urgenti per il contrasto del terrorismo, anche di matrice internazionale*» (artt. 1-10, eccetto l'art. 5), puntando innanzitutto a colpire le nuove modalità con cui si manifesta, da circa due anni, la minaccia terroristica e così a sanzionare il comportamento dei cd. *foreign fighters* o "lupi solitari", nonché i terroristi che da soli si addestrano via web e isolatamente agiscono, prevedendo un aggravante «*se il fatto è commesso attraverso strumenti informatici o telematici*» (nuovo co. 2 dell'art. 270 *quinquies* cp introdotto con il co.3, lett. "b", dell'art. 1 del dl).
Con l'art. 6 e l'art. 8 del dl n. 7/2015, vengono rispettivamente introdotte «*Modifiche al decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155*» (cioè al provvedimento già prima ricordato varato dopo gli attentati di Londra del 7 luglio 2005) riguardanti l'attribuzione di nuovi compiti alle Agenzie di Informazione (colloqui investigativi con detenuti ed internati al solo fine di acquisire informazioni per la prevenzione dei delitti con finalità terroristica di matrice internazionale) e al sistema delle garanzie funzionali degli appartenenti alle stesse Agenzie.

di rimuoverli. Presso il ministero dell'Interno sarà tenuto un elenco aggiornato dei siti in questione[12];

---

12 Ci si riferisce all' art. 2 del dl («*Integrazione delle misure di prevenzione e contrasto*»), secondo cui:

1. *Al codice penale sono apportate le seguenti modificazioni:*
   a) *all'articolo 302 (Istigazione a commettere alcuni dei delitti preveduti dai capi primo e secondo), primo comma, è aggiunto, in fine, il seguente periodo: «La pena è aumentata se il fatto è commesso attraverso strumenti informatici o telematici.»;*
   b) *all'articolo 414* (*Istigazione a delinquere*) *sono apportate le seguenti modificazioni:*
      1) *al terzo comma è aggiunto, infine, il seguente periodo*: «*La pena prevista dal presente comma nonché dal primo e dal secondo comma è aumentata se il fatto è commesso attraverso strumenti informatici o telematici.*»;
      2) *al quarto comma è aggiunto, infine, il seguente periodo*: «*La pena è aumentata fino a due terzi se il fatto è commesso attraverso strumenti informatici o telematici*».
2. *Ai fini dello svolgimento delle attività di cui all'articolo 9, commi 1, lettera b), e 2, della legge 16 marzo 2006, n. 146, svolte dagli ufficiali di polizia giudiziaria ivi indicati, nonché delle attività di prevenzione e repressione delle attività terroristiche o di agevolazione del terrorismo, di cui all'articolo 7-bis, comma 2, del decreto-legge 27.luglio.2005, n. 144, convertito, con modificazioni, dalla legge 31.luglio.2005, n. 155, l'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione, fatte salve le iniziative e le determinazioni dell' autorità giudiziaria, aggiorna costantemente un elenco di siti utilizzati per le attività e le condotte di cui agli articoli.270-bis e 270-sexies del codice penale, nel quale confluiscono le segnalazioni effettuate dagli organi di polizia giudiziaria richiamati dal medesimo comma 2 dell'articolo 7-bis del decreto-legge n. 144 del 2005, convertito, con modificazioni, dalla legge n. 155 del 2005.*
3. *I fornitori di connettività, su richiesta dell' autorità giudiziaria procedente, inibiscono l'accesso ai. Siti inseriti nell'elenco di cui al comma 2, secondo le modalità, i tempi e le soluzioni tecniche individuate e definite con il decreto previsto dall'articolo 14-quater, comma 1, della legge 3 agosto 1998, n. 269.*
4. *Quando si procede per i delitti di cui agli articoli 270-bis, 270-ter, 270-quater e 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 alcuno compia dette attività per via telematica, il pubblico ministero ordina, con decreto motivato, ai fornitori di servizi di cui all'articolo 16 del decreto legislativo 9 aprile 2003, n. 70, ovvero ai soggetti che comunque forniscono servizi di immissione e gestione, attraverso i quali il contenuto relativo alle medesime attività è reso accessibile al pubblico, di provvedere alla rimozione dello stesso. I destinatari adempiono. all'ordine immediatamente e comunque non oltre quarantotto ore dal ricevimento della notifica .In caso di mancato adempimento, si dispone l'interdizione dell'accesso al dominio internet nelle forme e con le modalità di cui all'articolo 321 del codice di procedura penale.*
5. *All'articolo 9, comma 9, del decreto legislativo 21 novembre 2007, n. 231, dopo le parole: «Guardia di finanza» sono inserite le seguenti: «nonché al Comitato di analisi strategica antiterrorismo».*

b) con l'art. 7 del dl n. 7/15, vengono previste «*Nuove norme in materia di trattamento di dati personali da parte delle Forze di polizia*» (se ne parlerà più avanti).

Gli interventi normativi del 2001, 2005 e 2015 hanno avuto una comune caratteristica: sono stati varati nella forma del decreto legge, quindi del provvedimento d'urgenza, venendo tutti convertiti in legge con grandissima maggioranza parlamentare.

Tuttavia, nonostante le logiche emergenziali da cui erano ispirate ed i tragici contesti in cui è avvenuta la loro approvazione, anche quelle leggi hanno rispettato i limiti che ogni democrazia deve darsi pur quando persegue esigenze di contrasto di gravi fenomeni criminali e di tutela della sicurezza.

Certamente anche in questi casi sono stati individuati dagli studiosi aspetti criticabili: la legge Pisanu del 2005 e quella del febbraio del 2015, ad esempio, diversamente dalle leggi del 2001, sembrano essersi adeguate alla filosofia degli interventi legislativi di molti altri Stati europei, in qualche modo tendendo a privilegiare le competenze degli apparati di *intelligence* ed a svincolare l'azione antiterrorismo dalla direzione e dal controllo degli uffici del pubblico ministero .

Ma in generale, come si è detto, si tratta di provvedimenti che appaiono coerenti con la scelta del nostro Paese, immediatamente seguita ai tragici eventi newyorkesi, di rinunciare a strumenti incompatibili con le regole di uno stato di diritto, ricercandosi invece:

- un'ulteriore progressione del processo di estensione ai procedimenti in materia di terrorismo di istituti nati per il contrasto della criminalità organizzata mafiosa;
- il rafforzamento, anche in ambito e per finalità extra-processuali, delle potestà di raccolta ed utilizzazione di informazioni utili alla penetrazione conoscitiva del fenomeno e all'accertamento dei reati, il tutto sotto il controllo dall'autorità giudiziaria e dunque in modo costituzionalmente sostenibile, pur in presenza di inevitabile compressione di correlate sfere di "privatezza" e libertà individuali.

Non si può neppure sottovalutare il fatto che, anche grazie alle leggi del 2001 e del 2005 (mentre per quella del 2015 si deve ancora attendere per valutarne le ricadute sulle indagini), l'Italia ha conseguito eccellenti risultati nell'attività di contrasto del terrorismo internazionale, tanto che, comparando i dati relativi ai processi celebratisi in questo settore in Europa, è risultato evidente che gli esiti dei procedimenti celebratisi in Italia sono tra i migliori, se consideriamo i numeri delle condanne definitive.

Si potrebbe anche prudentemente aggiungere un'ulteriore considerazione circa il fatto che l'Italia è fortunatamente rimasta esente da attentati e da stragi di matrice terroristica. L'unico tentativo di attentato ad opera di un kamikaze, infatti, è stato quello verificatosi a Milano nel 2009 ad opera di un libico[13], che ha ferito solo se stesso, perdendo una mano e la vista. Ciò è sicuramente frutto della grande professionalità della nostra polizia giudiziaria, ma non si deve escludere la ricaduta positiva di un sistema di leggi, dimostratosi insieme efficace e rispettoso dei diritti delle persone indagate. Tornano in mente le parole di una sentenza del 2004 scritta dal Presidente della Corte suprema israeliana: *«Guardando alla lotta dello Stato contro il terrorismo che si leva contro di esso, siamo convinti che, alla fine del giorno, una lotta condotta in conformità alla legge ne rafforzerà la forza e lo spirito. Non c'è sicurezza senza legge. L'osservanza delle previsioni della legge è un aspetto della sicurezza nazionale»*.

Eppure, nonostante questo quadro confortante, la magistratura italiana continua ad essere accusata di peccare di eccesso di garantismo: recentemente il giornalista Angelo Panebianco ha parlato di «*tratto timido dei magistrati*»[14] nel contrasto del terrorismo internazionale, quasi che abbassare il livello delle garanzie per indagati ed imputati sia condizione del successo contro questo tragico fenomeno criminale. Al giornalista ha dato ragione persino un *ex* sottosegretario all'Interno, il magistrato Alfredo Mantovano[15]. Francamente – e senza giri di parole – trovo queste posizioni inaccettabili.

Deve essere invece chiaro che la nostra democrazia non può tornare indietro di

---

13 Il 12 ottobre 2009, a Milano, attorno alle 7.30, all'ingresso della caserma «Santa Barbara» dell'esercito di piazzale Perrucchetti, proprio dinanzi al posto di controllo dell'accesso alla Caserma, il libico Mohamed Game, regolarmente soggiornante a Milano da anni, tentava di far esplodere una bomba rudimentale che portava con sé in una borsa. Si scopriva, poche ore dopo l'attentato, che era stato lui stesso a fabbricare l'ordigno, utilizzando sostanze chimiche da lui acquistate in un negozio di prodotti per l'agricoltura. Un soldato di guardia aveva fermato il libico che stava tentando di entrare in Caserma e lui aveva innescato immediatamente l'esplosivo che portava in una borsa. Fortunatamente, nessun militare era rimasto ferito, mentre l'attentatore aveva perso una mano e la vista. Non è emersa prova di collegamenti fra il libico e possibili centrali terroristiche internazionali: un classico caso di «terrorismo fai da te», di fanatici che si avvicinano alla pratica del terrore e che, attraverso internet, ne apprendono dogmi ed ideologia, così come, attraverso lo stesso mezzo, studiano le tecniche di fabbricazione in proprio di ordigni esplosivi. Una realtà ben conosciuta anche in altre parti d'Europa.

14 *Corriere della Sera*, 27 novembre 2015.

15 *Corriere della Sera*, 4 dicembre 2015.

un solo passo e che non possono esistere, come qualcuno teorizza, zone grigie nell'affrontare il terrorismo. Non si torna indietro neppure di un millimetro, per la semplice ragione che sui diritti non si tratta. È ovvio che ci troviamo di fronte a fenomeni nuovi, che comportano l'esistenza di scenari di guerra e non sono certo invidiabili coloro che devono prendere decisioni politiche riguardanti le opzioni possibili in quella direzione[16]. Ma qui stiamo discutendo di altro, della risposta istituzionale da dare ai fenomeni criminali che si manifestano, anche tragicamente, nei nostri territori.

Ed allora il punto di partenza non può che essere la constatazione del trovarci di fronte ad una forma di criminalità organizzata, pur se caratterizzata da un tratto speciale e da obiettivi particolari e diversi rispetto al terrorismo interno degli anni di piombo e anche rispetto a quello internazionale manifestatosi fino al 2011-2012. Si devono pertanto mettere in campo strumenti di investigazione certo affinati, sempre più specialistici ed in linea con le possibilità che anche a noi – oltre che ai terroristi – offre la modernità. Ma il tutto deve avvenire all'interno di una logica processuale, quella dell'accertamento delle penali responsabilità di chi si associa con complici mossi da identiche pulsioni e commette o progetta attentati, in cui sia previsto e rispettato – per l'indagato e l'imputato – l'esercizio pieno del diritto di difesa. Questo è il quadro in cui dobbiamo operare, quello che meglio tutela i cittadini ed in cui si collocano le valutazioni che seguono.

5. I dati personali, la loro diffusione e la loro raccolta a scopo investigativo

È stato già osservato da molti: viviamo in un sistema di relazioni sociali in cui servirsi delle tante tecnologie che facilitano la vita quotidiana implica che si lascino tracce di ogni tipo: si sa quando si è utilizzato un certo servizio, per quanto tempo, per quale ragione. Si conosce dove ci si è recati, con chi si è viaggiato e con quali soggetti si è eventualmente interagito; persino la spesa alimentare si può ordinare via internet senza necessità di recarsi al supermercato. Questo – e ben altro ancora – deve essere tenuto presente quando affrontiamo il discorso della raccolta dei dati personali e del loro utilizzo in chiave investigativa.

16 Peraltro, se è vero che atti di terrorismo possono essere realizzati anche in tempo e in zone di guerra, è anche vero che, in condizioni di guerra, trova applicazione il diritto bellico che vive innanzitutto nella Convenzione di Ginevra, nei suoi protocolli addizionali e trova ulteriori e più generali ragioni nel diritto umanitario.

È evidente, cioè, che siamo in presenza di un problema reale per ogni democrazia, poiché la necessità di tutela della privacy non può essere ridotta ad una frase di stile o riproposta con affermazioni di tipo retorico («*dobbiamo garantire la riservatezza dei dati personali*»), senza che alcuna Istituzione si faccia effettivamente carico delle conseguenze. Né è accettabile la ottusa obiezione giustificativa che si sente circolare quando si affronta questo tema, secondo la quale se non si ha nulla da temere non vi è ragione di preoccupazione per la raccolta di miriadi di tracce e per le conseguenti "schedature" delle nostre vite e di quelle degli altri.

Dobbiamo invece preoccuparcene perché, come ha scritto *Patrick* Radden Keefe[17], *«Viviamo in un mondo sommerso dai segnali. Partono dai nostri telefoni cellulari e di antenna in antenna arrivano al nostro amico che si trova, magari, in un altro Paese; il tutto nell'ordine di un secondo. L'aria intorno a noi e il cielo sopra di noi sono un'orgia di segnali. Intercettarli è facile come raccogliere la pioggia in una tazza".*

Insomma, se il continuo progresso sociale consentito dalle nuove tecnologie rappresenta ovviamente un'opportunità che chiunque deve poter sfruttare fino in fondo ai fini del miglioramento della qualità della propria vita, è necessario tenere presente che, almeno tendenzialmente, quanto più tali tecnologie sono sofisticate e quanto più sono utili e semplificano la vita quotidiana, tanto più il loro utilizzo implica che chi se ne serve lasci tracce elettroniche, cioè dati che, anche quando appaiono esteriori e poco invasivi, dicono in realtà molto circa le relazioni intrattenute da una persona. Se poi tali informazioni vengono conservate per periodi sempre più lunghi – come appunto le medesime tecnologie permettono a costi sempre inferiori – allora è possibile ricostruire l'intera rete delle relazioni sociali intrattenute da una persona nel tempo, arrivando in certi casi a ricordare di esse più di quanto gli stessi interessati siano a volte in grado di fare. Cresce così il numero delle banche dati e la loro interconnessione, sia in ambito pubblico che privato. E cresce contemporaneamente la capacità di memorizzare ed analizzare le informazioni raccolte in tali archivi elettronici secondo una estesa pluralità di criteri; ma la conservazione di una singola informazione può pesare sulla vita della persona a cui si riferisce.

Non si può neppure dimenticare che le banche dati cui i Servizi di informazione di molti Stati accedono per finalità di pubblica prevenzione dei rischi, come reso noto dai titolari dei *server* globali, sono ormai sempre più spesso enormi serbatoi predi-

17 *Echelon e il controllo globale,* Einaudi 2006.

sposti da soggetti privati, dunque orientate da logiche meramente economiche ed aziendali: persino una direttiva sulla protezione cibernetica del gennaio 2013 dell'allora *premier* Monti[18], per vari aspetti discutibile, rischia di favorire tale tendenza che estende, senza autorizzazione giudiziaria, i poteri delle Agenzie di informazione.

I problemi di sicurezza circa il trattamento di questi dati conseguentemente si dilatano tanto che l'assoluta inadeguatezza delle misure di protezione induce i Governi ad emettere provvedimenti ad hoc come quello appena citato ed a pensare a *manager* privati, anziché ad autorità con esperienze istituzionali, quali responsabili della cd. *cyber security* nazionale.

Da tutto ciò – sia ben chiaro – non si può certo pervenire alla inaccettabile conclusione secondo cui si dovrebbe rinunciare all'utilizzo degli strumenti investigativi che, come si è detto, la modernità ed il progresso tecnologico mettono a nostra disposizione.

Infatti – ed è ciò che qui interessa maggiormente – la conservazione crea un bacino di dati personali potenzialmente vastissimo, al quale le autorità giudiziarie e le forze di polizia possono attingere ricavando informazioni a fini di prevenzione o repressione dei reati e che consente loro di creare con maggiore facilità propri archivi elettronici per le medesime finalità.

Ciò è tanto più comprensibile, ove si pensi che i progressi della tecnologia non solo sono sfruttati dalle grandi organizzazioni criminali, ma determinano anche fenomeni delittuosi di più basso livello, capaci, però, di colpire gli interessi di una platea più vasta di cittadini di ogni Stato. Basti pensare ai *computer crimes* o, ancora, alla diffusione dei cosiddetti "furti di identità", legati al fatto che sempre più spesso si è rappresentati non già dalla propria immagine reale, ma da codici o segni identificativi trasmessi sulle reti di comunicazione elettronica, che possono essere duplicati ed utilizzati impropriamente da persone terze rispetto a quelle cui si riferiscono e appartengono. Crescono anche le possibilità di raccogliere dati personali senza che l'interessato ne abbia consapevolezza: si pensi, ad es., ai *cookies*. Alcuni dati sono necessari per garantire un utilizzo funzionale dei siti medesimi, ma altri determinano solo la raccolta di un gran numero di informazioni su chi naviga in rete, con particolare riferimento ai siti visitati, e quindi ai gusti e agli interessi di tali persone.

18 DPcm 24 gennaio 2013 del presidente del Consiglio *pro tempore* Monti: «Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale».

Ecco perché è ben comprensibile che gli organi di Polizia si attrezzino a loro volta, con personale specializzato, sfruttando le potenzialità offerte da questa nuova realtà tecnologica, sia per rispondere alle nuove condotte criminali sia per utilizzarle nelle indagini di tipo più tradizionale.

Proliferano così, anche a livello internazionale, le banche dati nate per queste finalità: quelle del Sistema-Schengen, di Interpol, di Europol e di Eurojust ne sono solo un esempio e proprio in virtù del complessivo accrescimento delle potenzialità dischiuse dall'utilizzo delle tecnologie a fini di polizia, alcuni legislatori e talune autorità amministrative si sono spinti fino a consentire alle forze incaricate della tutela della sicurezza pubblica un accesso quasi illimitato ai dati che vengono lasciati nel web da cittadini spesso inconsapevolmente.

Seconda parte

Le possibilità investigative che il sistema italiano prevede grazie a intercettazioni, raccolta dati, tracciamento e operazioni sotto copertura

6. Le possibilità che il sistema italiano prevede per l'analisi dei dati con finalità investigative

Ma è opportuno, a questo punto, passare brevemente in rassegna le possibilità che il sistema legislativo italiano pone a nostra disposizione per l'analisi dei dati che servono alle indagini. Mi riferisco a strumenti nuovi, ma anche a quelli tradizionali ed aggiornati, come intercettazioni telefoniche ed ambientali, intercettazioni preventive degli organi di polizia giudiziaria e delle agenzie di informazione, alle attività sottocopertura nei siti internet, acquisizione di tabulati e tracce varie di traffico di telefonia mobile etc... Se ne ricaverà la conclusione seguente: il sistema italiano di acquisizione dati è efficace e rispettoso dei principi vigenti in materia di tutela della riservatezza.

6.a. Le intercettazioni telefoniche, ambientali e dei dati telematici

Ancora oggi i principali strumenti di indagine utilizzati contro il terrorismo sono costituiti dalle intercettazioni telefoniche, telematiche (soprattutto per quanto riguar-

da il terrorismo di matrice religiosa e confessionale) e da quelle tra presenti (cd. ambientali).

Il regime dei presupposti e delle forme dei provvedimenti autorizzativi delle intercettazioni nell'ambito del contrasto del terrorismo prevede alcune deroghe al regime ordinario che già erano state previste, in ragione della loro particolare gravità, per i delitti di criminalità organizzata[19].

Con l'art. 3, co. 1, del citato dl 18 ottobre 2001, n. 374, convertito nella legge 15.12.2001 n. 438[20], in materia di «Disposizioni urgenti per contrastare il terrorismo internazionale», varato all'indomani dell'11 settembre, la predetta normativa è stata estesa al settore del contrasto al terrorismo, ponendo a disposizione della Polizia giudiziaria e dei Pubblici ministeri, contro fenomeni criminali di eccezionale gravità, una più ampia possibilità di utilizzo degli strumenti investigativi costituiti dalle intercettazioni delle conversazioni telefoniche ed ambientali. In particolare, è stata introdotta la possibilità di effettuare intercettazioni telefoniche, ambientali e di flussi informatici in presenza di *sufficienti* indizi di reato e di *necessità* delle intercettazioni (mentre il regime normale prevede la presenza necessaria di *gravi* indizi e di *assoluta indispensabilità* delle intercettazioni).

Si tratta di una scelta che ben si colloca nel solco di altre precedenti (e successive) caratterizzate dall'adozione di normativa speciale per fenomeni che determinano grave allarme sociale. La normativa in tema di intercettazioni telefoniche – come è noto – sottopone al controllo giurisdizionale la valutazione della ricorrenza dei presupposti autorizzativi dei provvedimenti in questione, il che determina una situazione ben diversa da quella conosciuta in altri ordinamenti ove siffatte valutazioni sono affidate ad Autorità politiche o di Polizia.

---

19 Al riguardo, la disciplina originaria è contenuta nell'art. 13, dl 13 maggio 1991, n. 152, convertito, con modificazioni, in l 12 luglio 1991, n. 203, recante provvedimenti urgenti in tema di lotta alla criminalità organizzata e di trasparenza del buon andamento dell'attività amministrativa.

20 Questo il testo della norma citata: «*Nei procedimenti per i delitti previsti dall'articolo 270-ter del codice penale* (ndr: «Assistenza agli associati») *e per i delitti di cui all'articolo 407, comma 2, lettera a), n. 4 del codice di procedura penale* (ndr: «delitti commessi per finalità di terrorismo internazionale o di eversione dell'ordinamento costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci, nonché delitti di cui agli artt. 270, terzo comma e 306, secondo comma, del codice penale»), *si applicano le disposizioni di cui all'articolo 13 del decreto-legge 13 maggio 1991, n. 152, convertito, con modificazioni, dalla legge 12 luglio 1991, n. 203*».

Appaiono privi di fondamento, peraltro, i rilievi a proposito dei presunti numeri elevati di intercettazioni telefoniche effettuate nel nostro Paese, fondati sulla comparazione dei dati relativi alle intercettazioni effettuate in altre zone d'Europa: sfugge del tutto, ai "censori" del nostro sistema, che in altri Stati europei (in Gran Bretagna soprattutto) gran parte delle intercettazioni telefoniche vengono effettuate dai Servizi d'informazione senza che ne sia possibile (oltre che l'uso processuale) conoscerne le quantità e gli esiti.

V'è da dire che rilievi e polemiche su tali presunti abusi non riguardano per nulla il settore delle indagini per terrorismo e ciò dimostra la strumentalizzazione delle esigenze di tutela della privacy (che dovrebbero valere per tutti) cui si assiste quando le intercettazioni pongono in evidenza rapporti corruttivi o altri reati dei cosiddetti "*colletti bianchi*".

Appare corretto, insomma, e quindi da non modificare (fatta salva ogni discussione tecnica sul regime del deposito e del rilascio di copie anche foniche delle registrazioni), il bilanciamento che il nostro sistema conosce tra le esigenze investigative proprie della fase delle indagini preliminari e la tutela del diritto alla riservatezza dei singoli.

6.b. Intercettazioni a mezzo "virus"

È noto anche che l'evoluzione della tecnologia ha determinato possibilità di utilizzo di nuovi strumenti di captazione come l'intercettazione, non ancora oggetto di assestamento giurisprudenziale, a mezzo di un particolare software (cd. *virus*), segretamente installato nel dispositivo da controllare: l'esigenza da preservare, in questi casi, è quella di evitare che l'attivazione di tutte le possibili funzionalità, ad esempio della videocamera o del microfono di uno *smartphone* grazie ad apposito comando inviato da remoto non finisca con il ledere diritti costituzionalmente garantiti, trasformandosi in uno strumento che venga ad accompagnare il soggetto in tutte le manifestazioni espressive della sua vita (privata, familiare, lavorativa), sottoponendolo ad un monitoraggio incontrollato, generalizzato e permanente al di fuori dei casi e dei modi previsti dalla legge ed in contrasto con i diritti di cui agli artt. 2, 13, 14 e 15 Cost. .

Le prassi e le linee guida operative elaborate in proposito dalle Procure della Repubblica, per quanto è noto, sono ispirate proprio alla necessità di prevenire tali rischi, che avevano indotto la VI sezione della Cassazione, con sentenza n. 27100 del 26 maggio scorso a dichiarare illegittime (con conseguente inutilizzabilità) le intercettazioni ambientali realizzate, a distanza, mediante immissione di *virus* informatici in uno

smartphone capaci di attivare microfono e videocamera. Secondo la Corte, infatti, in tal modo si consentono, oltre i limiti del decreto autorizzativo del gip e i presupposti del codice di rito relativi all'individuazione del luogo ove si stia svolgendo l'attività criminosa, captazioni ambientali ovunque, in qualsiasi luogo e contesto di trovi l'indagato. Di qui, quindi, l'esigenza di escludere l'ammissibilità di modalità investigative che, eludendo codice di rito e decreto del gip, consentano di fatto di sottoporre a un controllo totale, in qualsiasi luogo e momento, l'indagato, in violazione delle garanzie sancite dalla legge a tutela della libertà individuale nelle comunicazioni e nella sfera domiciliare. Tale indirizzo non sembrerebbe, tuttavia, consolidato dal momento che la stessa VI Sezione, il 10 marzo, ha investito delle questioni le Sezioni Unite che si devono ancora pronunciare.

Nel frattempo potrebbe anche pronunciarsi il legislatore nell'ambito della delega per la riforma della disciplina delle intercettazioni ora all'esame del Senato in seconda lettura. È auspicabile tuttavia che la norma sancisca garanzie non minori di quelle contenute nelle direttive di alcune Procure e, soprattutto, più efficaci di quelle previste dall'emendamento del Governo al ddl di conversione del dl 7/2015, stralciato poi in Aula con cui si intendeva modificare l'art. 266 *bis* del cpp. Tale emendamento, infatti, si limitava ad ammettere le intercettazioni da remoto quale ulteriore modalità di realizzazione delle operazioni captative, senza tuttavia introdurre cautele adeguate al grado di invasività che caratterizza tale strumento investigativo, per le sue stesse peculiarità

6.c. Le intercettazioni preventive ad opera della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza

Il tema delle intercettazioni preventive – con riferimento non solo alla disciplina regolatrice ma anche alle finalità cui sono mirate – è diventato di grande attualità almeno da quando il *New York Times*, alla fine del 2005, ha svelato il programma di intercettazioni segrete (*Terrorist Surveillance Program, Tsp*): si tratta delle intercettazioni telefoniche e di email effettuate durante il periodo dell'amministrazione Bush su cittadini americani, senza autorizzazione del giudice. Un sistema che, per alcune sue caratteristiche, si poneva come eccezione persino rispetto a quanto previsto dal già eccezionale *Patriot Act*. Una lapidaria sentenza del 17 agosto 2006 del giudice federale di Detroit, Anna Diggs Taylor, bollava come «anticostituzionali» le intercettazioni in questione, imponendone la immediata interruzione. Il giudice di Detroit le definiva «un gravissimo abuso di potere da parte del presidente George W. Bush», il quale «nel non rispettare le procedure legislative ha sicuramente violato il Primo e il Quarto emendamento della

Costituzione» [sulla tutela della privacy], nonché «la dottrina della separazione dei poteri e le leggi sulle procedure amministrative»[21]. Durante il processo, la Casa Bianca si era trincerata dietro «motivi di sicurezza nazionale» per rifiutarsi di fornire i dettagli del suo programma segreto e in una nota ufficiale il dipartimento della Giustizia, annunciando il ricorso contro la decisione del giudice, aveva definito il programma della National Security Agency (Nsa) «uno strumento cruciale che dà la possibilità di avere un sistema di preallarme per sventare o impedire attacchi terroristici». Il quotidiano newyorkese, inoltre, è stato accusato di avere recato un grave danno alla sicurezza dello Stato attraverso la pubblicazione dei suoi articoli di denuncia.

Appare opportuno, allora, richiamare la disciplina vigente in Italia in tema di intercettazioni preventive dimostrando che sia quelle ad opera delle forze di polizia giudiziaria che delle Agenzie di Informazione (se ne parlerà nel paragrafo successivo) sono regolate da disposizioni che comunque prevedono il controllo di un'Autorità giudiziaria.

In particolare, la disciplina delle intercettazioni preventive ad opera della Polizia di Stato, dell'Arma dei Carabinieri e del Corpo della Guardia di Finanza (in ordine alle quali si sta registrando un aumento delle previste richieste di autorizzazione ad opera degli organi di Polizia giudiziaria a ciò legittimati, probabilmente a seguito dell'emergere del fenomeno dei cosiddetti "*foreign terrorist fighters*", ancora da esplorare in Italia), è dettata dal già citato dl 18 ottobre 2001, n. 374 approvato dopo l'11 settembre e convertito con legge 15.12.2001 n. 438[22].

È bene ricordare che tali intercettazioni preventive, per quanto riguarda la materia del terrorismo:

- 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 costitu-*

21 La sentenza è stata emessa nel caso n. 06-CV-10204 dal predetto giudice dell'Eastern District of Michigan-Southern Division. La causa *(Aclu* v. *Nsa)* era stata promossa contro la Nsa, l'agenzia nazionale di sicurezza americana, dalla American Civil Liberties Union e da altre associazioni attive nel campo dei diritti umani, nell'interesse di molti cittadini americani che lamentavano di essere stati illegalmente sottoposti ad intercettazioni telefoniche in occasione di conversazioni intercorse per svariate ragioni con persone residenti in Medio Oriente.

22 Ci si vuol riferire, in particolare, all'art. 5, comma 1, che ha sostituito il testo previgente dell'art. 226 Norme di attuazione, coordinamento e transitorie del cpp.

zionale 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 autorizzate direttamente dal Procuratore della Repubblica (per un periodo iniziale di 40 gg. e con proroghe di 20 gg. ciascuna) e quindi non è richiesta l'adozione di provvedimenti autorizzativi o di convalida da parte del gip. Gli esiti, naturalmente, non possono costituire prova nei processi, ma possono dar luogo, oltre che ad attività di prevenzione, ad indagini vere e proprie.

La nuova formulazione della norma risente naturalmente della *ratio* generale di rafforzamento dell'attività di contrasto del terrorismo internazionale propria del decreto legge con cui è stata introdotta.

L'art. 5, infatti, anche in questi casi, estende all'attività di prevenzione dei delitti con finalità di terrorismo e di eversione (in generale individuati nel decreto attraverso il sistematico rinvio all'art. 407, comma 2, lett. a, n. 4, cpp) la possibilità di impiego di questo tipo di intercettazioni, in precedenza riservato al settore dei "delitti di mafia".

Va comunque specificato che a generali esigenze di garanzia e di rigorosa verificabilità della corrispondenza dell'agire preventivo ai limiti dell'autorizzazione ricevuta corrispondono l'obbligo, da parte dell'organismo richiedente, di motivare il rilascio delle autorizzazioni e delle successive (eventuali) proroghe ed il regime di documentazione dalle norme citate.

6.d. Le intercettazioni preventive dei Servizi di informazione istituiti con legge n. 801/1977 e riformati, quali Agenzie di informazione, con legge 124/2007, introdotte dal Decreto Pisanu

Con il citato Decreto-legge 27.7.2005 n. 144 (cd. "Decreto Pisanu"), convertito con legge 31 luglio 2005 n. 155, il Parlamento come già s'è detto, ha varato, in conseguenza delle stragi londinesi del luglio 2005, ulteriori norme al fine della più efficace prevenzione e repressione della minaccia terroristica di "matrice jihadista".

In particolare, ha introdotto la possibilità per i direttori dei servizi di informazione, sul presupposto di una delega del presidente del Consiglio dei ministri, di richiedere

di essere autorizzati dalle Procure generali presso le Corti d'appello allo svolgimento di intercettazioni preventive (oltre che all'acquisizione di tabulati telefonici e telematici).

Il testo originario del decreto assegnava al Procuratore generale presso la Corte di cassazione la relativa potestà autorizzatoria, ma tale previsione è stata opportunamente eliminata in sede parlamentare per l'evidente rischio di contaminazione dell'ufficio requirente di legittimità con le logiche tipiche della valutazione prognostica dell'opportunità dell'adozione di invasive tecniche di raccolta informativa.

Al procuratore generale presso la Suprema Corte erano stati dunque sostituiti per l'esercizio di quelle funzioni di controllo i Procuratori generali presso le Corti di appello, una soluzione comunque assai insoddisfacente, trattandosi di uffici che ordinariamente non dispongono del *know-how* necessario per valutare la potenziale interferenza delle attività informative dei Servizi di sicurezza nelle ordinarie attività di investigazione.

Successivamente, con l'art. 12 co. 1 della legge 7 agosto 2012 n. 133, il potere autorizzativo è stato attribuito al Procuratore generale presso la Corte d'appello di Roma, con conseguente attenuazione dei predetti rilievi critici, che non avrebbero più avuto ragione di essere se tale potere – come era logico – fosse stato attribuito, con il dl n. 7/2015 al Procuratore nazionale antimafia ed antiterrorismo competente per il coordinamento investigativo in questi settori.

Risultano comunque rispettati i parametri affermati dalla giurisprudenza della Corte Edu di Strasburgo (di cui si parlerà appresso), tra cui la presenza di un vaglio giudiziale (sia pur non giurisdizionale) che deve però essere un vaglio intrinseco, che possa sindacare l'effettiva ricorrenza dei presupposti prescritti dalle legge per tale tipo di intercettazioni, incluse le proroghe, a carico dei soggetti da sottoporre a controllo.

Una delle caratteristiche di questa nuova normativa può facilmente individuarsi nel rafforzamento, anche in ambito e per finalità extra-processuali, delle potestà di raccolta ed utilizzazione di informazioni utili alla penetrazione conoscitiva del fenomeno, con conseguente estensione dei poteri di intervento autonomo dei Servizi di informazione istituiti con legge n. 801/1977, poi riformati con la legge 3.8.2007, n. 124 e quindi denominati Agenzie di informazione[23].

23 Per quanto ampiamente noto, va ricordato, ai soli fini che qui interessano, che la disciplina dell'attività e delle competenze delle Agenzie di informazione è regolata dalla legge 3 agosto 2007, n. 124 («Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto»). La legge del 2007

Naturalmente tocca all'Autorità giudiziaria titolare del potere di autorizzazione – cioè la Procura generale della Corte d'appello di Roma – la verifica del rischio di inutili e dannose duplicazioni di attività delle Agenzie rispetto a quelle di Polizia giudiziaria, anche perché, ai sensi dell'art. 23 co. 7 della legge 3 agosto 2007 n. 124: *«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»*

6.e. Tabulati e tracce telefonia mobile

La questione relativa all'acquisizione della documentazione integrale del traffico storico degli apparati telefonici (i cd. tabulati telefonici), visto il grande rilievo probatorio dei dati che è possibile trarne, ha impegnato in passato la giurisprudenza, prima che venisse dettagliatamente regolata con legge.

I tabulati telefonici, come è noto, sono sostanzialmente documenti di natura informatica (ormai solo raramente di natura cartacea) elaborando sistematicamente i quali è possibile desumere i dati relativi alle relazioni personali (desumibili dalla individuazione di conversazioni telefoniche tra numero chiamante e numero chiamato, dall'accertamento dei rispettivi intestatari o degli utilizzatori di tali numeri), alla loro

---

(che ha cancellato la precedente risalente al 1977) ha modificato innanzitutto le denominazioni dei due Servizi "segreti": il Sismi (Servizio per le informazioni e la sicurezza militare) ed il Sisde (Servizio per le informazioni e la sicurezza democratica) oggi si chiamano rispettivamente Aise (Agenzia informazioni e sicurezza esterna) e Aisi (Agenzia informazioni e sicurezza interna).
Nei settori di rispettiva competenza, la ricerca ed elaborazione di tutte le informazioni utili è affidata all'Aise in vista della difesa dell'indipendenza, dell'integrità e della sicurezza della Repubblica dalle minacce provenienti dall'estero ed all'Aisi per difendere la sicurezza interna della Repubblica e le istituzioni democratiche ... da ogni minaccia, da ogni attività eversiva e da ogni forma di aggressione criminale o terroristica. Oltre ad altre funzioni, ad entrambi i Servizi è poi affidato il compito di individuare e contrastare le attività di spionaggio dirette contro l'Italia e quelle volte a danneggiare gli interessi nazionali, ma mentre l'Aise opera al di fuori del territorio nazionale, l'Aisi lo fa all'interno di esso. La legge prevede poi un organo di coordinamento dei due servizi, il Dis (Dipartimento Informazioni per Sicurezza), nonché modalità di controllo politico sulla loro attività, affidato al Comitato parlamentare per la sicurezza della Repubblica (Copasir), equivalente del vecchio Copaco previsto dalla legge abrogata del 1977.

intensità (desumibili dalla durata e frequenza delle conversazioni) e, in alcuni casi, per quanto ovviamente concerne la telefonia mobile, al posizionamento geografico di coloro che conversano ed agli orari di tali posizionamenti (desumibili dal luogo ed orario in cui gli apparati "agganciano" i segnali trasmessi dalle antenne destinate alla copertura delle aree di servizio della telefonia mobile all'atto dell'effettuazione delle conversazioni telefoniche).

Come ben si comprende, trattasi di uno strumento investigativo che, contrariamente alle intercettazioni (il presupposto delle quali è sempre l'attualità della conversazione), consente di rivolgere uno sguardo investigativo anche al passato, scontando come unico limite quello della conservazione temporale dei dati presso le compagnie telefoniche.

Più in generale, si può dire che, negli ultimi 20 anni, lo sviluppo delle nuove tecnologie ha indotto e portato tanti e tali mutamenti negli ordinamenti giuridici nazionali e sovranazionali da provocare una sorta di vero e proprio passaggio ad una nuova "era giuridica", sol che si consideri l'attività normativa che ne è via via scaturita e che ha esteso ai gestori l'obbligo conservazione dei dati di riferimento di ogni comunicazione, telefonica e telematica, per finalità di accertamento e repressione dei reati.

Anche in questo caso è con il cd. "Decreto Pisanu" del luglio del 2005 (delle cui linee generali si è già detto) che il legislatore è intervenuto sull'obbligo di conservazione dei dati del traffico telefonico e telematico, creando un nuovo regime di acquisizione più agile, più snello, che attribuisce al pm nuove possibilità.

Con l'art. 6, comma 3, in particolare, sono state apportate modifiche (per quanto riguarda tipologia dei dati, tempi di conservazione e modalità di acquisizione degli stessi) all'articolo 132 del decreto legislativo 30 giugno 2003, n. 196, recante il Codice in materia di protezione dei dati personali.

Successivamente, con il Decreto legislativo 30 maggio 2008 n. 109 («Attuazione della direttiva 2006/24/Ce riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/Ce») sono intervenute ulteriori modifiche al contenuto dell'art. 132 Codice privacy:

- l'art. 2 contiene specifiche indicazioni sui tempi di conservazione dei dati di traffico (da un minimo di sei mesi a un massimo di due anni);
- l'art. 3 definisce le *«Categorie di dati da conservare per gli operatori di tele-*

fonia e di comunicazione elettronica», in relazione ad alcuni specifici servizi offerti dai fornitori (telefonia di rete fissa e telefonia mobile, accesso a internet, posta elettronica in internet e telefonia via internet), sempre *per le finalità di accertamento e repressione dei reati.*

È così possibile individuare gli autori di una comunicazione, loro localizzazione, volume e durata del traffico telefonico ed altri dati nell'ipotesi in cui i dati stessi risalgono fino a 24 mesi antecedenti. L'acquisizione è possibile presso i fornitori con decreto motivato del pubblico ministero (anche su istanza del difensore, dell'imputato, dell'indagato, della persona offesa e delle altre parti private) per qualsiasi reato (si pensi alla contravvenzione di molestia) e in assenza del benché minimo *standard* probatorio[24]. Il difensore di indagato ed imputato può chiedere direttamente al fornitore, invece, i dati relativi alle utenze intestate al proprio assistito con le modalità dell'art. 391 *quater* cpp (*ex* art. 132, comma 3 d.lgs n. 196).

Sono clamorosi alcuni esempi e casi concreti di indagini effettuate attraverso l'acquisizione dei dati di telefonia mobile tratti dai cd. tabulati: basti pensare alle indagini sul sequestro di Nasr Osama Muostafa Hassan, *alias* Abu Omar (Milano, 17.2.2003) che hanno portato alla condanna definitiva di 26 imputati statunitensi di cui 25 appartenenti alla Cia (gran parte dei quali identificati attraverso l'analisi dei movimenti di 17 telefoni cellulari, individuati dopo analisi dei dati relativi ad oltre 10.700 presenti nella zona e nella fascia oraria del sequestro) ed a quelle che hanno determinato la cattura in Roma di Osman Hussein, uno degli attentatori di Londra (fatti del 7 luglio 2005) il cui telefono risultava essere stato localizzato in Francia e poi agganciato al suo ingresso in Italia mentre si recava a Roma. Ma molti altri casi – e più recenti – potrebbero essere citati, anche in relazione ad indagini relative a settori criminali diversi da quello del terrorismo.

Ma l'uso di telefoni mobili, i cd. "cellulari", e le tracce che lasciano possono risultare utili anche agli indagati ed ai loro difensori, in quanto acquisibili nell'ambito

24 Prima delle modifiche conseguenti al d.lgs n. 109/2008, era consentita, solo per indagare su delitti connotati da particolare gravità (delitti di cui all'art. 407 co. 2, lett. "a" del cpp) o sui delitti in danno di sistemi informatici e telematici (per i quali l'utilizzo di questo strumento di indagine appare praticamente indispensabile), l'acquisizione degli stessi dati – in base a provvedimento del giudice emesso su istanza del pubblico ministero, del difensore dell'imputato, dell'indagato, dell'offeso e delle altre parti private – per un periodo risalente fino al doppio, e cioè 48 mesi**,** purché ricorresse un livello probatorio qualificato (sufficienti indizi). Nei casi di urgenza il provvedimento di acquisizione poteva essere emesso dal pm, con successiva convalida da parte del Giudice.

di attività investigative difensive o tramite istanza rivolta al pubblico ministero[25], per provare il fondamento di un alibi addotto e, dunque, la propria non colpevolezza: un indagato potrebbe dimostrare, ad esempio, di essersi trovato in luogo diverso da quello di consumazione del delitto attribuitogli. O meglio, potrebbe provare la localizzazione in area diversa dal teatro del delitto del telefono mobile da lui normalmente utilizzato, con onere ulteriore di provare che egli ne sia stato, in quel momento, l'utilizzatore.

Le prescrizioni fin qui descritte potrebbero peraltro variare a seguito di una modifica del quadro normativo europeo, tanto più probabile dopo la declaratoria di illegittimità della direttiva 2006/24/Ce (di modifica della direttiva 2002/58) da parte della Corte di giustizia con la sentenza *Digital Rights* dell'8 aprile 2014. La Corte ha infatti ritenuto che la particolare invasività di questo strumento investigativo (che per sua natura comporta la conservazione dei dati di ciascun cittadino, per consentire eventualmente l'acquisizione in sede processuale dei soli dati degli indagati) non fosse, nella direttiva, contemperata da correttivi adeguati, in base alla gravità del reato per il cui accertamento si proceda, al termine di conservazione dei dati stessi e al vaglio giurisdizionale (o comunque di un'Autorità terza) che, nella direttiva, non era previsto come necessario. Tali carenze integrerebbero quindi, secondo la Corte, una violazione del principio di proporzionalità tra diritto alla protezione dati ed esigenze investigative.

6.f. Le operazioni di tracciamento e di positioning *(localizzazione) dei telefoni mobili*

I dati esterni alla comunicazione possono essere non solo *raccolti* quando ormai la comunicazione è avvenuta da tempo, e quindi sotto forma di documento "storico" (come avviene, appunto, con l'acquisizione dei tabulati), ma possono anche essere acquisiti in tempo reale, ovvero in contemporanea alla comunicazione.

Questa operazione, che fornisce alle autorità inquirenti i dati esterni alla comunicazione contemporaneamente alla fonia, viene definita "tracciamento" e altro non è che un effetto tangibile dell'eccezionale evoluzione tecnologica di quella che, con le vecchie centrali elettromeccaniche, si chiamava "blocco" della chiamata: attraverso il "blocco" – cioè l'arresto degli organi di commutazione del circuito su tutta la rete –

25 Ai sensi dell'art. 358 cpp, infatti, il pm è tenuto a svolgere accertamenti su fatti e circostanze a favore della persona sottoposta ad indagini.

si poteva materialmente seguire il tracciato della comunicazione all'interno della rete stessa e così individuare la linea del soggetto chiamante.

La tecnica del "blocco della chiamata" è stata utilizzata soprattutto negli anni '70 nelle indagini concernenti i sequestri di persona a scopo di estorsione; anzi, prima che tale tecnica di investigazione diventasse nota ai criminali, furono numerosi i casi di "telefonisti" di bande di sequestratori arrestati mentre, in lunghe conversazioni telefoniche, contrattavano con le famiglie del sequestrato o con loro emissari il pagamento del riscatto e le sue modalità.

La prestazione del "tracciamento", pur avendo una propria autonomia logica, materiale e giuridica, viene tipicamente fornita dall'operatore (destinatario del provvedimento dell'Autorità giudiziaria) unitamente a quella di "intercettazione" dei contenuti effettivi della comunicazione; dati esterni e contenuti vengono poi trasmessi agli impianti installati nella rocura della Repubblica per la loro conservazione nel tempo.

Ma può anche accadere che gli organi di indagine dispongano la sola attività di tracciamento, ovvero che le due prestazioni siano disgiunte.

Ad esempio, l'evenienza ricorre quando si è in possesso del solo numero seriale identificativo dell'apparecchio telefonico mobile in senso fisico (il cd. codice Imei): in questo caso il tracciamento del terminale è un passaggio obbligato per identificare in tempo reale la Sim Card a esso associata, che potrà poi essere oggetto di ulteriore intercettazione di fonia.

Un'ulteriore progresso tecnologico nell'attività di tracciamento è rappresentata dalla tecnica del cd. *positioning* (o di localizzazione).

Si è già detto, che i gestori telefonici conservano i dati relativi ai servizi forniti ai loro clienti per il periodo massimo consentito dalle norme di legge. Ma i tabulati di traffico telefonico si riferiscono *esclusivamente* ai dati che, originariamente, sono autorizzati a trattare per le necessità di natura "commerciali" (telefonate, sms, etc.) e per gli apparati mobili comprendono l'indicazione della stazione radio impiegata al momento della effettuazione o della ricezione della chiamata.

Essi non annoverano pertanto alcuna informazione nel momento in cui il terminale mobile, anche spostandosi, non effettua o riceve alcuna chiamata.

Sempre su preventiva richiesta dell'Autorità giudiziaria, per i telefoni cellulari – quando sono regolarmente connessi ad una rete – può essere acquisita l'informazione circa la loro collocazione geografica (la precisione dipende dalla elaborazione di una

serie di fattori) anche in assenza di chiamate: tale servizio, realizzabile anche non in presenza di eventi di comunicazione, differisce pertanto da quello di intercettazione o di tracciamento che si può attivare solo in presenza di eventi di comunicazione.

6.g. L'attività sottocopertura. In particolare quella rispetto ai siti internet

I dati utili per le indagini giudiziarie, sempre più frequentemente, possono essere anche desumibili dal *web*[26], dalle *banche dati on line* (che costituiscono vere e proprie "collezioni" di informazioni specializzate, generalmente accessibili via internet e tramite abbonamento) e dalle *e-mails* (posta elettronica tra persone ovunque localizzate)

Orbene, anche l'attività sottocopertura rispetto ai siti internet è oggi possibile e ben disciplinata in Italia.

Con l'art. 4, c. 2 del citato dl n. 374/2001, conv. nella l 438/2001 (*post* 11 settembre), che costituisce la risposta speculare rispetto all'accertato utilizzo della rete internet da parte dei gruppi terroristici, si è infatti previsto 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.

---

26 *Internet*, come è noto, sta diventando il principale "media" attraverso cui è possibile ottenere e diffondere gratuitamente documenti ed informazioni di ogni genere, anche se non certificate: anche i gruppi criminali, in particolare le associazioni con finalità terroristiche vi fanno spesso ricorso per il raggiungimento dei loro obiettivi. A tal proposito, Gilles Kepel, in un articolo pubblicato su *La Repubblica* del 27.7.05, sottolineava che *«il Web è stato preso in ostaggio dai gruppi estremisti, che lo usano per aggirare la censura di Stato, accelerando la circolazione delle idee, delle informazioni, delle parole d'ordine jihadiste. S'è creato, così, un nuovo spazio planetario, un'Umma digitale»*.

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.

Questa previsione denota la preoccupazione del legislatore di disciplinare attentamente attività astrattamente suscettibili di determinare una massiccia invasione della *privacy* dei cittadini. Infatti, si tratta di operazioni che possono essere effettuate solo dagli ufficiali di Polizia giudiziaria appartenenti agli organismi investigativi della Polizia di Stato, dell'Arma dei Carabinieri specializzati nell'attività di contrasto al terrorismo e della Guardia di Finanza specializzati nelle attività di contrasto al finanziamento del terrorismo anche internazionale.

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*».

A proposito di questo tipo di attività, deve essere infine citata anche la Legge 16/03/2006 n. 146 di ratifica della convenzione delle Nazioni Unite contro il crimine organizzato transnazionale**,** in base alla quale (art. 9) i nostri reparti specializzati possono, anche avvalendosi di ausiliari, 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. Gli stessi ufficiali di polizia giudiziaria, previa autorizzazione, possono attivare siti nelle reti, realizzare e gestire 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. Con il medesimo decreto sono stabilite altresì le forme e le modalità per il coordinamento, anche in ambito internazionale, a fini informativi e operativi tra gli organismi investigativi.

Questa possibilità è molto importante, anche se l'attività sottocopertura nei siti internet e la necessità di efficaci interventi di monitoraggio dei siti stessi costituiscono tipica materia da disciplinare a livello di accordi internazionali, essendo noto, ormai, che il modo di agire e far propaganda dei gruppi terroristici è mutato negli ultimi anni ed è oggi

difficile che, come avvenuto in passato, siano a tal fine utilizzate – in modo clandestino e magari nascosto anche a chi ne è responsabile – aree particolari di luoghi religiosi o di formazione culturale islamica. La propaganda, infatti, si svolge ormai via web ed è ben possibile, per quella via, anche l'auto-addestramento a pratiche violente e terroristiche .

Può essere utile, in proposito, riportare quasi integralmente il contributo del generale Mario Parente, espertissimo investigatore, già comandante del Ros dei Carabinieri[27]:

«*Il web si pone dunque all'attenzione quale mezzo d'elezione per la diffusione del messaggio jihadista. Può raggiungere chiunque e ovunque, avviando processi di radicalizzazione violenta nell'assoluto anonimato.*

Ne consegue per l'individuazione dei potenziali terroristi la necessità di una penetrante attività di monitoraggio di quei siti internet che rivestono un ruolo essenziale nei processi di radicalizzazione … ora si può diventare terroristi in totale autonomia, frequentando siti jihadisti e visionando i filmati propagandistici prodotti da Al Qaeda e, più recentemente, dallo Stato Islamico. … omissis…

Sotto il profilo dell'azione di contrasto, nuove opportunità sono costituite dal monitoraggio dei social media o social networks, divenuti ormai lo strumento principale di diffusione sia del materiale di propaganda "ufficiale" prodotto dalle organizzazioni terroristiche, sia dei messaggi e dei contenuti multimediali prodotti dagli stessi foreign fighters o aspiranti tali. La loro potenza comunicativa è enorme e soddisfa l'esigenza, comune a molti foreign fighters, di condividere le proprie esperienze di guerra. I combattenti documentano con post ed immagini sui loro profili facebook le fasi di preparazione al viaggio, l'arrivo in zona di operazioni, la loro vita quotidiana e le loro impressioni sui combattimenti. Tra l'attivista che si trova in Europa ed il militante recatosi in una zona di guerra per combattere il jihad, si instaura un rapporto molto stretto e di profonda conoscenza che si traduce in un reciproco rafforzamento dei rispettivi propositi. Il combattente trova motivazione e supporto per continuare la propria "missione", mentre i suoi interlocutori possono trovare stimoli e motivazioni per seguirlo o per condurre il loro jihad in Occidente.

Sebbene le organizzazioni terroristiche facciano uso di una vastissima gamma di social media in relazione alle diverse funzioni offerte, Facebook risulta senza dubbio

27 Relazione tenuta nel corso del Seminario sulla minaccia terrorista organizzato dalla Fondazione Icsa presso il Centro Alti Studi per la Difesa (Roma, 18 febbraio 2015).

quello di maggior interesse dal punto di vista investigativo, ponendosi come principale ambiente virtuale di radicalizzazione violenta per i sostenitori di Al Qaeda e dello Stato islamico. Facebook ha assunto in particolare un ruolo di rilievo nel reclutamento dei foreign fighters per il conflitto siriano, consentendo il contatto con i potenziali volontari, convincendoli a partire e comunicando loro le istruzioni per raggiungere il teatro di guerra.

Il maggiore successo di Facebook quale veicolo di radicalizzazione, rispetto ad altri social media quali Twitter, YouTube, Instagram, è dovuto anche ad alcune sue peculiarità. Prima di tutto, offre una gamma ampia e diversificata di modalità di espressione, per mezzo di testi, foto, audio e video. I contenuti possono essere ordinati cronologicamente ed inoltrati alla propria rete di contatti, corredati da commenti. Esistono poi numerose modalità per adattare lo strumento alle singole e specifiche esigenze di riservatezza: una chat anonima integrata, la possibilità di creare gruppi tematici aperti o chiusi, la graduazione di livelli diversi di "amicizia" cui corrisponde un diverso grado di conoscibilità delle informazioni del profilo e, infine, un sistema di ricerca automatico di altri account affini, basato sui dati personali.

È stato verificato come il ricorso alle diverse funzioni offerte da Facebook vari in relazione all'evoluzione del processo di radicalizzazione. Semplificando, si possono distinguere quattro fasi.

Nella prima si manifesta l'adesione a un'ideologia radicale, con la pubblicazione in un proprio profilo generalmente non anonimo di espressioni di supporto testuali o visive a organizzazioni terroristiche.

Una seconda fase vede l'utente impegnato nella ricerca attiva di altri individui ideologicamente affini, con cui stabilire una rete di amicizie o con cui interagire nell'ambito di gruppi tematici estremistici.

Successivamente, in una terza fase, si approfondiscono le relazioni con gli individui più radicali, utilizzando canali di comunicazione non pubblici, quali chat anonime, rendendosi invisibili al di fuori della cerchia di amicizie selezionata.

L'eventuale quarta fase è caratterizzata dall'uso di strumenti di comunicazione clandestini per comunicare con gli altri membri del gruppo virtuale, anche nell'ottica di pianificare attività terroristiche.

Il monitoraggio dei profili Facebook consente pertanto di seguire un soggetto potenzialmente a rischio nel suo processo di radicalizzazione, acquisendo progressivamente indizi sul suo eventuale coinvolgimento in attività terroristiche.

Il grado di anonimità scelto è in genere direttamente proporzionale al processo di radicalizzazione. Vengono così utilizzati profili con dati personali anonimi, i post di natura estremistica vengono cancellati o resi visibili solo alla rete occulta di amici fidati. Anche un profilo "vuoto", privo di post di natura terroristica può risultare sospetto, soprattutto, se i contenuti terroristici sono stati di recente cancellati o privatizzati. Il cambiamento può essere indicativo dell'esigenza dell'utente di mantenere clandestini i propri contatti e comunicazioni, in relazione per esempio alla decisione di pianificare un attentato terroristico.

In tale ambito, l'analisi dei collegamenti rappresenta senza dubbio lo strumento più efficace a disposizione dell'investigatore per la ricostruzione di una rete. La quantità di informazioni che caratterizza e definisce i collegamenti su Facebook è tale da riproporre nel mondo virtuale scenari e dinamiche analoghi a quelli che avevano caratterizzato la struttura reticolare delle cellule terroristiche in Europa prima dell'esplosione del fenomeno homegrown. Se fino alla metà del decennio scorso esistevano cellule ed individui collegati nel mondo fisico, in modo tale che da una cellula fosse possibile risalire alle altre, oggi quegli stessi rapporti possono essere riprodotti dalle "amicizie" stabilite su Facebook.».

6.h. Le novità introdotte con il Decreto legge antiterrorismo del 2015

Si tratta di un intervento normativo che, al di là di aspetti definitori comunque non secondari, introduce alcune disposizioni su possibilità di accesso, controllo e oscuramento del web e anche sulla conservazione dei dati.

Con l'art. 7 del dl n. 7/15, vengono previste «Nuove norme in materia di trattamento di dati personali da parte delle Forze di polizia», introducendo modifiche all'articolo 53 («Ambito applicativo e titolari dei trattamenti») del decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali).

Le novità consistono, da un lato, nella parte meramente definitoria di cui al co. n. 1[28] e, dall'altro, nel fatto che nel co. 2 si prevede l'estensione della originaria riserva di

28 Art. 53-Ambito applicativo e titolari dei trattamenti.

1. Agli effetti del presente codice si intendono effettuati per finalità di polizia i trattamenti di dati personali direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché.di polizia giudiziaria, svolti, ai sensi del codice di procedura penale,

legge, fino a ricomprendervi regolamenti e decreti, quali atti che possano contenere indicazioni sui trattamenti di dati ai quali – purché effettuati per finalità di polizia – non si applicano gli articoli 9, 10, 12, 13 e 16, da 18 a 22, 37, 38, commi da 1 a 5; da 39 a 45; e da 145 a 151 del codice per la protezione dei dati personali, contenenti alcuni obblighi come informativa, notificazione ecc. .

Queste modifiche al citato codice tendono dunque a semplificare la disciplina del trattamento di dati personali da parte delle forze di polizia. Fino ad oggi la norma prevedeva un regime agevolato solo per i trattamenti specificamente previsti da disposizione legislativa. Con il dl n. 7/2015, invece, tra le fonti suscettibili di legittimare la raccolta di dati a "regime agevolato", oltre alla legge ordinaria che richiede tempi tecnici più lunghi, sono previsti anche le norme regolamentari e lo specifico decreto del Ministro dell'interno ricognitivo dei vari trattamenti svolti per fini di prevenzione e repressione dei reati.

Ovviamente, sarà necessario garantire l'equilibrio complessivo di questo nuovo sistema, coinvolgendo il Garante per la protezione dei dati personali, ma intanto il legislatore mostra attenzione rispetto all'obiettivo di renderne possibile l'utilizzo ricercando un accettabile equilibrio con le più volte richiamate esigenza di tutela dei diritti dei cittadini costituzionalmente garantiti.

6.i. Giudizio di sintesi sul sistema italiano

La "rassegna" normativa che precede consente dunque di affermare che nel nostro sistema disponiamo di strumenti efficienti e ben disciplinati per indagare in vari settori criminali, tra cui quello del terrorismo, utilizzando i dati che intercettazioni ed intrusioni nel web consentono di conoscere e di raccogliere.

E sono strumenti che le nostre forze di polizia specializzate sanno bene usare, come eccellenti risultati in molte delicate indagini hanno dimostrato.

Anche la magistratura – sia consentito dirlo – ha mostrato da tempo attenzione rispetto a questi strumenti di analisi e d'indagine, non solo perché è tenuta a rilasciare – su richiesta dagli organi competenti – autorizzazioni motivate per le attività prima descritte, ma anche perché ha costituito in molte procure, in modo del tutto spontaneo

per la prevenzione e repressione dei reati.

ed in relazione alle indagini per terrorismo, varie banche di dati giudiziari, gestite da colleghi esperti, incaricati anche di mantenere i collegamenti con gli altri uffici inquirenti. Questo avvenne ben prima che venisse estesa la operatività della Banca dati della Direzione nazionale antimafia anche al campo del terrorismo.

Né è stato trascurato il dovere di tutela della privacy. Anzi la magistratura vi ha prestato costantemente attenzione, spesso anche in assenza di auspicati interventi legislativi: mi permetto di dire che all'interno della Procura di Torino, che ho l'onore di dirigere, è stato varato il 15 febbraio scorso un provvedimento che obbligherà i magistrati dell'ufficio ad attivare le procedure di cancellazione dei dati inutilizzabili, oppure irrilevanti e insieme sensibili ai sensi del Codice per la protezione dei dati personali (art. 4, lett. "d" del d.lgs 30 giugno 2003, n. 196). Il tutto senza lesione del diritto di difesa poiché gli avvocati potranno prendere conoscenza del contenuto di dati e conversazioni di quel tipo (non di riceverne copia) e di intervenire dinanzi al giudice nella procedura di cancellazione attivata dal pubblico ministero. Ed analoghi provvedimenti sono stati e saranno adottati da altre procure della Repubblica.

Le intercettazioni e la raccolta di dati rilevanti, dunque, sono ben disciplinate in Italia e sono state ben utilizzate in chiave investigativa.

Terza parte

Il panorama europeo, l'erronea centralità dei mega-dati e dell'*intelligence*, la perdurante sofferenza della cooperazione giudiziaria. Il necessario confronto e rispetto con il mondo islamico

7. Il panorama internazionale e la propensione alle inutili raccolte dei mega-dati

Se però si guarda al panorama internazionale ed a come viene altrove pensato ed attuato l'utilizzo di questi strumenti in chiave antiterroristica se ne possono ricavare delusioni variamente motivate.

Vorrei partire da un ricordo personale: anni fa, e per molto tempo, ho partecipato ad incontri e scambi di informazioni presso la sede di Eurojust a L'Aia. Mi capitò,

pertanto, di partecipare ad un incontro in cui un rappresentante dell'amministrazione americana spiegava a noi europei un sistema di raccolta-dati che gli Stati Uniti avevano adottato negli scenari di guerra in cui all'epoca operavano: ci raccontò che ogni volta che le forze statunitensi americane occupavano un qualsiasi centro urbano, anche di modeste dimensioni, sito in zone di guerra, raccoglievano tutti i numeri telefonici in possesso degli abitanti, indipendentemente dall'esistenza di sospetti di attività terroristiche a loro carico, al fine del successivo inserimento in una gigantesca banca dati antiterrorismo. Personalmente domandai a che cosa fosse mai servito un sistema così esteso e privo di criteri di selezione a monte o se avesse mai consentito risultati positivi. Seguirono risposte vaghe ed una reazione di stupore anche da parte di colleghi di altri Paesi europei.

E rammento pure – a sostegno della inutilità di raccolte così indiscriminate – che il giorno di Natale del 2009, un giovane nigeriano, Umar Farouk Abdul Mutallab, tentò di farsi esplodere sul volo Delta Airlines Amsterdam-Detroit: nonostante gli apparati di sicurezza americani possedessero molti dati su di lui e il padre stesso ne avesse denunciato a un'ambasciata Usa la progressiva radicalizzazione e un lungo soggiorno nello Yemen a scopo di addestramento, egli era in possesso di regolare visto che autorizzava il suo ingresso negli Usa. Infatti si imbarcò sull'aereo con i suoi documenti e solo la prontezza di un passeggero impedì che si facesse esplodere in volo. Insomma, persino un dato derivante da una dettagliata ed esplicita denuncia, se confuso in una miriade di dati, si perde e non serve a nulla, perché si fa eccessivo affidamento sulle massicce raccolte di dati, quasi che esistesse una relazione diretta fra il numero di informazioni "archiviate" ed i risultati investigativi conseguibili, un assioma privo di fondamento

Un argomento su cui non si deve abbassare l'attenzione, in particolare, è quello della raccolta dei *Passenger Name Records* (Pnr): si tratta – come è noto – delle notizie personali relative ai passeggeri in partenza verso varie destinazioni dai Paesi dell'Unione europea, per affari o per turismo, che secondo alcuni strateghi dell'antiterrorismo dovrebbero essere raccolti in gigantesche banche dati ed ivi custoditi: si tratterebbe di sacrifici accettabili in nome della maggior sicurezza da garantire al mondo occidentale (a quest'idea si ispira del resto la direttiva europea su cui, poco dopo Charlie Hebdo, si è raggiunto l'accordo politico).

La fiducia in questo strumento si è manifestata in modo imponente – specie al fine di rendere più sicuri gli aeroporti e gli aerei civili europei – all'indomani della scoperta risalente al 2006, ad opera delle forze di polizia britanniche coadiuvate da investiga-

tori statunitensi, di piani di attentati da commettersi in contemporanea su diversi voli transatlantici. Ancora una volta, però, ai primi annunci su quelle indagini, non fecero seguito notizie confortanti sull'esito dei procedimenti giudiziari riguardanti i piani criminali asseritamente scoperti che, come molti degli addetti ai lavori sanno, risultarono ampiamente ridimensionati. Ma la circolazione dei cittadini europei, da quel momento, è sottoposta a monitoraggi e ad una invasiva raccolta di dati personali.

Si spiega, allora, perché nel suo rapporto dell'11 settembre del 2008, l'organizzazione *Statewatch* denunciò «*lo tsunami digitale*» che all'epoca stava per scatenarsi sull'Europa: tecniche e tecnologie di sorveglianza su spostamenti e transazioni delle persone, sui beni da loro posseduti o utilizzati al fine di dar luogo alla creazione di ulteriori banche dati utilizzabili per la "lotta al terrore". È la stessa filosofia posta alla base del controllo dei dati bancari tramite Swift (dall'inglese *Society for Worlwide Interbank Financial Telecommunication*), rispetto alla quale anche l'Unione europea non cessa di prestare attenzione, sempre nella prospettiva di ritenere legali ed irrinunciabili, nella lotta al terrorismo, il controllo e la classificazione di mezza umanità, trascurando la dimensione del "*danno collaterale*" che ne può derivare per le persone in tutto il mondo: un sacrificio inaccettabile anche in nome della lotta al terrorismo.

Sempre a proposito della acritica fiducia nella raccolta indiscriminata di dati come strumento utile contro il terrorismo, va ricordato quanto è venuto alla luce negli ultimi anni con il caso Wikileaks-Julian Assange del 2010, con il caso Datagate del 2013-2014, scaturito dalle rivelazioni di E. Snowden e del soldato Manning, con la rivelazione del 2015 delle intercettazioni dell'NSA ai danni di *leaders* politici europei e dell'inizio 2016, sempre dell'NSA, in danno di esponenti di precedenti Governi italiani, nonché sulle estese acquisizioni di dati riguardanti cittadini italiani. Molti autorevoli commentatori hanno già posto in evidenza la grave ed inaccettabile lesione del diritto alla privacy emersa con quei casi, ma lo sdegno è durato poco e persino importanti politici "spiati" in vari Stati europei hanno preferito che il silenzio prevalesse.

Se dopo queste vicende gli Usa abbiano compreso il valore reale della protezione dati, soprattutto nel suo rapporto con la sicurezza, è ancora presto a dirsi[29].

29 Sarà in proposito interessante valutare, documenti alla mano, l'esito della controversia che, sulla base di un provvedimento della Corte federale di Los Angeles, oppone l'Fbi e la Apple, che ha rifiutato di "sbloccare" l'i-phone di Syed Rizwan Farook, autore della cd. strage di San Bernardino, coperto da un sistema di criptazione. Alla fine di marzo, peraltro, si è appreso che l'Fbi avrebbe trovato il modo di

A chi, ciononostante, sostiene che sia legale ed utile nella lotta al terrorismo raccogliere milioni di dati, così controllando e classificando mezza umanità (qualcuno è arrivato a sostenere l' obbligo di identificazione degli utenti di internet, con possibilità di verifica della veridicità dei dati dichiarati e di sanzioni per le violazioni!), si deve rispondere ripetendo il mantra opposto, cioè che la concentrazione di miriadi di dati indistintamente e perennemente raccolti – è provato – non è mai servita a nulla e che la strada da percorrere, invece, è quella che permette l'accumulo mirato e selettivo di dati per un tempo limitato e l'accesso agli stessi grazie ad un provvedimento motivato dall'Autorità giudiziaria.

Tra l'altro, accumulare dati significa anche moltiplicare i sospetti, rinunciare ad una *intelligence* mirata. Ed affidarsi alle "macchine" induce a rinunziare a quelle complesse politiche differenziate che sono in grado di affrontare il difficile problema di garantire la sicurezza nel rispetto dei diritti, significa non valorizzare quell'intelligenza investigativa che, unica, consente di contrastare e reprimere le gravi forme di criminalità con cui si è dovuta confrontare la nostra società.

Non sufficientemente esplorata, invece, è l'altra faccia della medaglia: ammesso che tali lesioni siano accettabili in democrazia – e non lo sono – si può almeno affermare che così estese raccolte di dati siano effettivamente utili in chiave di lotta al terrorismo e di tutela della sicurezza dei cittadini?

In tale prospettiva di analisi, è sufficiente provare ad interrogarci su come, in concreto, l'estensione delle banche dati prive di seria logica selettiva, possa essere utile in chiave preventiva o repressiva.

Sul piano della prevenzione: come sarebbe stato possibile, con la raccolta di mega-dati che pure a tanti sembra indispensabile, prevenire una strage come quella del Bataclan a Parigi del 13 novembre scorso ed altre ancora? Come?

Nel gennaio del 2015 il Garante europeo della protezione dati (*European Data Protection Supervisor*), Buttarelli, ribadendo la necessità del pieno rispetto, anche nel contrasto del terrorismo internazionale, dei diritti individuali e dei principi fondamentali delle nostre democrazie, ha prima citato la sentenza dell'8 aprile 2014 della

sbloccare l'i-phone, grazie ad una "terza parte" coinvolta nella procedura e senza l'aiuto della Apple, la quale aveva, a sua volta, anticipato che – in questo caso – avrebbe chiesto di conoscere il metodo utilizzato (Televideo, 29.3.2016, pag. 154.01).

Corte di giustizia europea (che, come già anticipato, intervenendo nei casi C-293/12 e C-594/12, ha dichiarato la invalidità della Direttiva 2006/24 del Parlamento europeo sul tema della *Data Retention*[30] in quanto incompatibile con il principio di proporzionalità riconosciuto dagli articoli 7 e 8 della Carta dei diritti fondamentali) e ha poi – quasi provocatoriamente (*ndr: commento di chi scrive*) – domandato in quale modo la raccolta di Pnr potrebbe essere rilevante contro la minaccia terroristica e se esiste una qualche dimostrazione che una possibile direttiva sulla raccolta dei Pnr avrebbe potuto ostacolare l'attacco alla sede del Charlie Hebdo a Parigi. *«Quale sarebbe, allora, il valore aggiunto di ulteriori categorie di dati Pnr per combattere criminalità e terrorismo?»*[31].

Ed il presidente del Garante italiano per la protezione dei dati personali, on.le Antonello Soro ha scritto, a proposito della invocata necessità «*... della cessione, da parte delle compagnie aeree alle autorità inquirenti, delle informazioni riguardanti i passeggeri (cd. Pnr)*» che deve essere ribadita «*l'esigenza di un giusto equilibrio tra sicurezza e privacy*» prevedendo *«tempi e modalità di conservazione dei dati ragionevoli e proporzionati alle esigenze delle indagini per i reati più gravi»*. Ed ha poi ricordato che ogni possibile disciplina della materia deve rispettare *«... il principio di proporzionalità su cui la Corte di giustizia ha modulato il bilanciamento tra libertà e sicurezza, nella sentenza di aprile sulla data retention*[32]*, sottolineando l'esigenza di un'adeguata selezione del materiale investigativo, che non può certo fondarsi sulla pesca a stra-*

30 Direttiva 2006/24/Ce del Parlamento europeo e del Consiglio dell'Unione europea del 15 marzo 2006, adottata dopo gli attentati di Madrid del 2004 e di Londra del 2005, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modificava la direttiva 2002/58/Ce del 12 luglio 2002.

31 Intervento del 27 gennaio 2015, a Bruxelles, dinanzi alla Commissione Libe del Parlamento europeo che lo aveva invitato ad intervenire sul tema *Counter-terrorism, De-Radicalisation and Foreigni Fighters*.

32 La sentenza dell'8 aprile 2014 della Corte di giustizia europea, intervenendo nei casi C-293/12 e C-594/12, ha dichiarato la invalidità della Direttiva 2006/24 del Parlamento europeo sul tema della *Data Retention* in quanto incompatibile con il principio di proporzionalità riconosciuto dagli articoli 7 e 8 della Carta dei diritti fondamentali. La Direttiva 2006/24/Ce del Parlamento europeo e del Consiglio dell'Unione europea del 15 marzo 2006, adottata dopo gli attentati di Madrid del 2004 e di Londra del 2005, riguarda la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e modificava la direttiva 2002/58/Ce del 12 luglio 2002.

scico nelle vite degli altri. Perché non è sostenibile democraticamente né utile alle indagini. Un'efficace azione di prevenzione del terrorismo deve dunque selezionare (con intelligenza, appunto) gli obiettivi "sensibili" in funzione del loro grado di rischio e fare della protezione dati una condizione strutturale della cyber-security»; occorre, dunque, una «*... adeguata selezione dei dati realmente utili ai fini d'indagine ... a dimostrazione ... della sinergia (tutt'altro che antagonismo!) tra protezione dati e sicurezza, tanto più in un mondo che, per fortuna, ha visto cadere ormai ogni frontiera e che, dopo le rivelazioni del Datagate, non può più considerare la privacy come un lusso cui rinunciare, in nome di una malintesa idea di sicurezza.*».

Ma le banche dati di cui stiamo parlando non servono neppure sul piano repressivo, posto che già disponiamo degli strumenti utili alle indagini: per esempio, se viene consumato un attentato e gli investigatori vogliono conoscere l'identità di coloro che hanno viaggiato verso la città dove l'attentato si è verificato, la possono accertare perché le compagnie aeree conservano i dati per un sufficiente periodo di tempo; se vogliono conoscere tutti i dati dei telefoni mobili che hanno operato nella zona dell'attentato fino a 24 mesi prima, possono ottenerli grazie alla previsione di tale periodo di conservazione cui sono obbligati – almeno in Italia – gli operatori di telefonia. Possono ottenere questo ed altro, in maniera efficace e rapida, grazie al nostro sistema ed ai motivati provvedimenti emessi dall'autorità giudiziaria, cui, in armonia con la normativa internazionale, è devoluto il controllo sulla effettiva utilità, pertinenza e proporzionalità dell'accesso ai dati ed informazioni quando richiesto dalla polizia giudiziaria.

Il rischio per la società futura, allora, non riguarda più soltanto l'equilibrio tra garanzie e sicurezza, ma investe la sua stessa configurazione: torneremo alla *"società del borgo*[33]*"*, che non conosceva la *privacy?*

E *«che cosa diventa la libertà di circolazione* – si domanda Stefano Rodotà[34] – *quando video-sorveglianza e localizzazione attraverso i telefoni mobili si trasformano in un guinzaglio elettronico che permette di seguire e registrare ogni nostro spostamento? Che cosa diventa la libertà di comunicare quando si registrano e si conservano per anni, peraltro in condizioni di precaria sicurezza, tutti i dati di traffico relativi a telefonate, posta elettronica, accessi ad Internet?»*.

---

33 L'efficace immagine è di Gianni Buttarelli, segretario generale del Garante per la protezione dei dati personali, nel Convegno dell'Assintel su *Data Retention, Privacy e Criminalità* (Milano, 16.1.06).

34 S. Rodotà: *Dove finiscono i diritti in un Paese di intercettati?* (*La Repubblica*, 25.7.06).

Voglio ulteriormente approfondire il tema della inutilità della raccolta indiscriminata di dati personali, citando un'audizione istituzionale che si tenne nell'ottobre del 2013: ricordo che, al fine di fornire dati affidabili e non soggettivi, interpellai colleghi delle principali Procure distrettuali impegnate in indagini sul terrorismo internazionale, nonché responsabili della Polizia di Stato e dei Carabinieri appartenenti a reparti specializzati in quel settore, per sapere se mai, come si andava dicendo in quel periodo, vi fosse stata una qualche ricaduta positiva sulle indagini dalle mitiche mega banche-dati di cui da sempre si parla. La risposta fu assolutamente negativa: mai catturati latitanti o sventati attentati, come dagli Usa si faceva sapere, senza fornire particolare alcuno, nel pieno delle tensioni createsi dopo la emersione delle notizie sulle intercettazioni effettuate "in danno" di *leaders* politici europei. Anzi, qualcuno degli addetti ai lavori da me consultati sostenne che ne fossero derivati solo danni ed intralci alle indagini. Risposta che formalmente feci mia nel corso dell'audizione, spiegando che le nostre forze di Polizia giudiziaria hanno saputo cogliere eccellenti risultati lavorando – peraltro su autorizzazione della magistratura, come le leggi italiane impongono – su dati numericamente più contenuti e logicamente orientati, quali mail ed sms tra soggetti ragionevolmente sospettabili, comunicazioni personali intervenute in certi ambiti territoriali, accessi a specifici siti on line etc.

Ecco perché, se mi è permesso dirlo, ho sempre trovato i commenti critici delle Autorità Garanti per la tutela della privacy, a livello nazionale o europeo, del tutto condivisibili anche dalla prospettiva del pubblico ministero .

Ed ecco anche perché veicolare in Europa il sistema italiano sarebbe sufficiente ad ottenere risultati positivi, un sistema che consente, come già si è detto, possibilità sicuramente soddisfacenti di utilizzo delle intercettazioni telefoniche ed ambientali, nonché di acquisizione di dati di telefonia e di altra origine, salvaguardando il diritto alla protezione dati nella consapevolezza che su di esso si misura la qualità della democrazia e da esso dipende la nostra libertà.

È proprio in questa direzione che va elaborata in Europa una normativa uniforme in materia di intercettazioni telefoniche, ambientali nonché di conservazione dei dati relativi al traffico telefonico e telematico. Da un lato, cioè, si dovrebbero uniformare gli *standard* legislativi di autorizzazione e di durata delle intercettazioni telefoniche ed ambientali, dall'altro si dovrebbe finalmente affrontare il tema della cd. *data retention* (ancora soggetta a discipline nazionali molto diverse, in taluni casi penalizzanti), in ogni caso prestando attenzione alla reale efficacia delle misure limitative del diritto alla riservatezza, condizione della loro accettabilità.

8. Un caso eclatante di pronuncia della Corte di giustizia dell'Unione europea: la sentenza *Safe Harbour*

Il tema in discussione non è ovviamente ignoto alla giustizia europea che se ne è occupata sotto varie angolazioni.

Non possiamo dimenticare, ad esempio, la sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015[35] che, pur non direttamente concernente il contrasto del terrorismo, costituisce un importante punto di riferimento: la Corte, infatti, ha dichiarato invalida la decisione della Commissione europea del 26 luglio 2000 n. 2000/520/Ce che aveva ritenuto adeguato il livello di protezione dei dati personali garantito dagli Stati Uniti d'America nel contesto del cd. regime di «*Safe Harbor*». Tale regime riguardava il sistema di trasferimento negli Stati Uniti dei dati di molte società private. «*Di fronte ad una politica aggressivamente ripiegata sulla sola economia, sono i giudici che cercano di mantenere viva l'Europa dei diritti»,* ha scritto S. Rodotà[36], con riferimento a quella sentenza ed all'accertata violazione del diritto fondamentale alla tutela della privacy.

Si può ipotizzare che proprio la sentenza *Safe Harbour* e la consapevolezza dell'impossibilità di discriminare gli utenti di una realtà globale come quella digitale in ragione della loro nazionalità abbiano determinato negli Stati Uniti il disegno della legge denominata *Judicial Redress* (approvata definitivamente il 10 febbraio e promulgata dal Presidente Obama il 24 febbraio 2016), che estende ai cittadini europei alcune garanzie per i trattamenti dei loro dati da parte delle autorità statunitensi.

Purtroppo, non pare destinato ad essere cancellato il *double standard* previsto dalla riforma dell'*intelligence* in chiave antiterrorismo (*Freedom Act*), che pur introducendo alcune garanzie rispetto alle acquisizioni di dati personali per fini di sicurezza, lascia fuori, in gran parte di tale settore, i cittadini non americani.

35 Sentenza relativa alla causa C-362/14, Maximillian Schrems vs. Data Protection Commissioner.

36 S. Rodotà: *Internet e privacy. C'è un giudice in Europa che frena gli Usa* (*La Repubblica*, 12 ottobre 2015).

9. Sentenze della Corte europea dei diritti dell'uomo sulla illegittimità dei poteri attribuiti alle Agenzie di informazione. Sentenze delle Corte costituzionali tedesca e portoghese sul divieto di accesso incontrollato dei Servizi ai dati di telefonia mobile

Neppure alle Agenzie di informazione, però, può essere attribuito un indiscriminato ed incontrollato potere di raccolta ed utilizzo di "mega-dati".

La Corte europea dei diritti dell'uomo lo ha affermato in due recenti sentenze:

- la sentenza del 4 dicembre 2015 della Grand Chamber sul caso Roman Zakharov v. Russia (n. 471443/06) con cui la Russia è stata condannata per il potere riconosciuto ai Servizi segreti ed alla polizia di effettuare sorveglianza ed intercettazioni degli apparati di telefonia mobile in modo arbitrario ed abusivo. Tra i principi affermati vi è anche quello della necessità di consentire all'interessato di sapere, sia pur una volta che siano cessate le esigenze di prevenzione, di essere stato sottoposto a controllo;
- la sentenza del 12 gennaio 2016 sul caso Szabò e Vissy v. Ungheria (n. 37138/14) con cui anche l'Ungheria è stata condannata per le intercettazioni telefoniche e telematiche da parte dei Servizi di intelligence, rese possibili da una legge antiterrorismo del 2011.

Tale normativa difetterebbe infatti, secondo la Corte, di garanzie sufficienti per impedire abusi, consentendo la captazione delle comunicazioni di cittadini, da parte del comparto antiterrorismo della polizia: in presenza di generiche esigenze di contrasto al terrorismo, senza dunque specifici presupposti individualizzanti a carico del soggetto da intercettare, tali da restringere l'ammissibilità della captazione ai soli casi e alle sole persone effettivamente attinte da rischi per la sicurezza nazionale; su mera autorizzazione del Ministro della giustizia (in assenza di alcun vaglio giurisdizionale o comunque di un potere esterno e diverso da quello esecutivo); per un periodo non determinato nel massimo, essendo illimitato il numero di proroghe suscettibili di concessione; in assenza di alcuna procedura che consenta al cittadino intercettato di avere contezza, sia pur una volta cessate le esigenze di sicurezza, di essere stato soggetto a controllo e, se del caso, contestarne la legittimità;

Sono anche molto importanti, ai fini che qui interessano, due sentenze, rispettivamente, della Corti costituzionale tedesca e portoghese**:**

- la sentenza n. 31/2013 della Corte costituzionale tedesca, nel dichiarare parzialmente illegittima la legge sulla raccolta e lo scambio di dati per fini antiterrorismo ha, in particolare, ribadito il principio di separazione delle informazioni raccolte per fini di *intelligence* da quelle utilizzabili per fini di polizia e la necessaria tassatività dei presupposti legittimanti i poteri di acquisizione dei dati personali da parte della Agenzie, precisando peraltro come, a fronte della estensione di tali poteri, sia ancor più necessaria un'adeguata supervisione da parte delle Autorità di protezione dati;

- la sentenza della Corte costituzionale portoghese del 28 agosto 2015 ha dichiarato la illegittimità del potere di accesso dei Servizi segreti ai tabulati degli apparati di telefonia mobile, previsto dalla normativa antiterrorismo. La Corte ha ritenuto che l'acquisizione di tali dati, in assenza di un vaglio giurisdizionale autorizzativo, analogo a quello del processo penale, costituisce «un'ingerenza particolarmente grave nelle comunicazioni private», la cui riservatezza è garantita dalla Carta fondamentale. La legge – la cui applicazione era limitata ai casi di lotta contro il terrorismo, traffici internazionali o rischi per la sicurezza dello Stato – era stata approvata il 22 luglio precedente a larga maggioranza e prevedeva comunque l'autorizzazione, sia pur di mera legittimità, di una commissione *ad hoc* composta da tre magistrati requirenti scelti dal Consiglio superiore della magistratura portoghese.

Le sentenze in questione consentono una riflessione, peraltro favorita dalla interpretazione logica e giuridica delle competenze delle Agenzie di informazione: va evitata ogni possibile confusione tra le loro competenze e quelle della polizia giudiziaria.

Le funzioni, delle Agenzie di informazione, infatti, non sono investigative in senso giudiziario ed anzi, la legge n. 124/2007, che in questo ricalca quella del '77, prevede che se le Agenzie entrano in possesso di notizie di reato devono obbligatoriamente comunicarle alla polizia giudiziaria per le indagini di competenza, salvo un provvedimento del presidente del Consiglio che ritardi tale comunicazione (art. 23, commi 6,7 ed 8 della legge). E la polizia giudiziaria, come è noto, deve a sua volta comunicare al pubblico ministero ogni notizia di reato «senza ritardo».

Orbene, appare assolutamente necessario, in tema di contrasto del terrorismo sul piano giudiziario, rispettare attentamente queste differenti finalità e competenze, pur se – ovviamente – le Agenzie di informazione e le forze di polizia giudiziaria dovranno sapersi tra loro coordinare e le notizie che dalle une perverranno alle altre ben potranno essere sviluppate ed assumere eventualmente forma legale nel corso delle indagini;

ma è capitato frequentemente, in molte parti di Europa, di verificare lo svilupparsi di pericolose tendenze, proprie di altri sistemi: da un lato, polizia e magistratura tendono troppo spesso a trasferire nei processi, senza alcuna attività di riscontro investigativo, dati e notizie di fonte meramente informativa; dall'altro, i Servizi di informazione tendono a ritenersi titolari di funzioni investigative in senso proprio, assimilabili, cioè, a quelle della polizia**.**

Quello che, però, si vuol qui ribadire ancora una volta, confermando le valutazioni che precedono, è che anche al fine di prevenire i rischi per la sicurezza dello Stato e dei cittadini, il che rientra nelle competenze proprie delle Agenzie, le indiscriminate raccolte di dati di cui qui si parla non servono a nulla.

Ne deriva che è necessario un efficace controllo su questo tipo di attività che, per restare al sistema italiano, non può che spettare al Copasir, cioè all'istituzione titolare, sul piano politico, del potere di vigilanza sull'attività delle Agenzie di informazione. Un controllo che, a dire il vero, ove si consideri anche l'assenza di rilievi sull'utilizzo ed estensione del segreto di Stato cui si è assistito negli ultimi anni (sanzionato dalla Corte europea dei diritti dell'uomo con la sentenza del 23 febbraio 2016 sul caso Abu Omar), dovrebbe decisamente essere più incisivo. Il Garante per la protezione dei dati personali ha peraltro stimolato proprio il Copasir all'esercizio dei propri poteri di impulso e garanzia rispetto all'operato dei Servizi italiani, così da garantirne la legittimità anche rispetto alle attività di collaborazione con le agenzie di *intelligence* straniere.

10. Le criticabili prospettive dell'Europa nel contrasto del terrorismo internazionale: si punta solo su mega-dati e *intelligence* senza preoccuparsi del malfunzionamento della cooperazione internazionale

A proposito dell'*intelligence*, è criticabile la quasi assoluta unidirezionalità degli indirizzi europei, secondo cui la risposta efficace al terrorismo sta tutta nel rafforzare le attività di intelligence. Quotidianamente si leggono sulla stampa articoli che parlano, sin dai titoli, del nuovo e decisivo patto dell'Unione europea contro il terrorismo, quello incentrato sul coordinamento tra i Servizi segreti. Vorrei fare una premessa per evitare equivoci connessi a "criticità" rilevate in passato: credo fortemente alla funzione delle Agenzie di informazioni in ogni democrazia. Ma ho anche più volte affermato,

e chiedo scusa se mi ripeto, che – al di là del citato problema della confusione tra differenti competenze – è la sinergia tra le tutte le istituzioni e le forze in campo che deve essere perseguita, non il mero rafforzamento delle cosiddette attività di *intelligence*, senza contemporaneamente operare per rendere effettiva la cooperazione giudiziaria internazionale, di cui sono protagonisti la magistratura e le forze di polizia tradizionali. Basti pensare, ad esempio, alle difficoltà, spesso insuperabili, che si manifestano quando si vogliono utilizzare come prove in un processo gli elementi raccolti dai Servizi nelle loro attività ed alle diverse prospettive con cui si affrontano questi problemi: rammento persino che un'esponente del *Crown prosecution servic*e inglese, nel corso di un importante incontro tra esperti di terrorismo organizzato a Parigi, alla fine di aprile del 2015, sostenne che spesso, raccolte le prove a carico di persone sospettate, bisogna chiedersi se esiste un interesse pubblico a punire chi ne è attinto!

Le difficoltà nel far funzionare la cooperazione giudiziaria – sia ben chiaro – dipendono anche dalle differenze ordinamentali che esistono tra gli Stati europei, per cui è difficile che in ogni parte d'Europa possa essere accettato che la direzione della polizia giudiziaria – come in Italia – spetti ai pubblici ministeri, con conseguente comune elaborazione delle strategie investigative e sottrazione delle medesime alle scelte politiche. Ed allo stesso modo è certamente sconosciuto alla maggioranza degli Stati europei il principio – per noi irrinunciabile – di assoluta indipendenza del pubblico ministero rispetto al potere esecutivo.

Se, invece, si opera principalmente attraverso i servizi di *intelligence*, ontologicamente portati a non mettere in comune le notizie, è chiaro che la guida della loro azione non potrà che essere politica. Di qui le scelte prevalenti in favore dei Servizi care ai Governi europei, talvolta anche a scapito delle efficienza operativa e della qualità dei risultati, con l'aggiunta di un'ulteriore ricaduta negativa: le regole secondo le quali operano i Servizi – diversamente da quelle scritte nei codici e nelle Convenzioni – non possono che essere, per definizione, segrete, dunque diverse tra loro ed incontrollabili, tali da alimentare spesso metodi d'azione a dir poco criticabili.

Ma se questi sono problemi di struttura costituzionale che in sé riguardano i rapporti tra magistratura, polizia giudiziaria ed Esecutivo, un altro importante ostacolo si frappone al funzionamento della cooperazione internazionale: spesso, cioè, si manifestano enormi resistenze nel mettere in comune, a fini investigativi, le notizie ed i dati davvero utili. Ciò costituisce un vero paradosso in quanto, da un lato, si proclama l'importanza della raccolta e dello scambio di dati ed informazioni per rafforzare la cooperazione giudiziaria contro il terrorismo ed altre forme pericolose di criminalità e,

dall'altro, non si scambiano, fra gli Stati europei (e spesso neppure fra le diverse forze di sicurezza all'interno di uno Stato membro dell'Unione), i dati che sarebbero davvero utili a tale scopo, «*evidentemente perché molti si ritengono proprietari esclusivi delle notizie importanti*»[37].

Esiste insomma il problema della "compartimentazione" tra Stati che contraddice la stessa presunta *ratio* delle banche dati e compromette la cooperazione internazionale: solo di rado, infatti, chi entra in possesso di una notizia utile contro il terrorismo ne mette immediatamente al corrente gli altri Stati. Ancora non sappiamo, ad esempio, sulla base di quali elementi si affermi con certezza che i terroristi dell'IS si finanzino con il grande traffico di stupefacenti o in altro modo.

Non appare ancora sufficientemente diffusa in Europa, dunque, l'attitudine culturale a forme di cooperazione effettiva. Per personale esperienza di chi scrive la cooperazione ha invece funzionato egregiamente nei rapporti tra Italia, Germania e Spagna, non a caso tre Paesi che hanno rispettivamente conosciuto il terrorismo interno delle Brigate Rosse (e di altri gruppi di estrema sinistra ed estrema destra), della *Rote armee fraktion* (Raf) e dell'Eta, riuscendo a sviluppare anticorpi efficaci (dall'analisi delle strategie e del "pensiero" di quei gruppi, alla specializzazione investigativa ed allo scambio immediato delle notizie utili che ancora oggi servono.

Insomma, l'Europa deve essere capace di contrapporre alla libertà di azione dei gruppi criminali terroristici ed alla loro capacità di proselitismo attraverso il web, un'altrettanto agile e globale azione investigativa e di repressione che comporta fiducia reciproca nel grado di affidabilità dei rispettivi ordinamenti (pur se sensibilmente diversi), abbandono di visuali particolaristiche ed attenuazione dell'impatto negativo che frontiere giuridiche e culturali determinano sull'azione repressiva di così gravi fenomeni delittuosi.

Certo, abbiamo registrato in passato scelte virtuose dell'Unione europea come l'adozione del mandato d'arresto europeo, la costituzione delle Squadre investigative comuni (peraltro solo da poco recepita in Italia[38]), la Decisione quadro del Consiglio

37 Così il Segretario generale dell'Interpol, Ronald Noble, il 19.11.2005, in un *meeting* di studio tenutosi presso la N.Y. University.

38 La possibilità di costituire squadre investigative comuni sovranazionali esiste in Italia solo a seguito della recentissima approvazione del **d.lgs 15 febbraio 2016**, n. 34 ma l'Unione Europea ha

dell'Unione europea sulla definizione dell'atto di terrorismo, la creazione di Eurojust ed Europol. Ma proprio per questo, verrebbe da dire, non vi è tanto bisogno di nuove Convenzioni, di nuove risoluzioni e decisioni quadro, di nuovi istituti giuridici ed istituzioni comunitarie, quanto di far funzionare effettivamente e con convinzione gli strumenti già esistenti. Del resto, già «esistono almeno sette banche dati europee: quella del sistema Schengen, Eurodac per le impronte digitali, quella per la concessione dei visti, quella delle dogane, quella in materia di asilo, quelle di Europol ed Eurojust»: qualcuna funziona più o meno bene, altre sono praticamente inutilizzate. Ma comunque – come ha detto il Garante europeo per la privacy Gianni Buttarelli[39] – «sono cattedrali nel deserto che non comunicano tra loro». Ed a ciò si aggiunga che il sistema di collegamento fra casellari giudiziari (Ecris) è (da poco) operativo solo per i cittadini europei, ma non prevede ancora i nomi dei condannati/ricercati da Paesi terzi (reperibili in parte sul sistema Interpol).

Questo allora è il cuore della questione: l'energia spesa a livello internazionale soltanto nella direzione di moltiplicare interventi di facciata, Dichiarazioni quadro e Risoluzioni è fine a se stessa. Lo dico da cittadino oltre che da magistrato. E mi augurerei che le autorità politiche italiane, nelle sedi che contano, anche sulla spinta di ciò che affermano i nostri autorevoli garanti per la tutela della privacy, assumessero un ruolo guida nel dibattito europeo, chiedendo convergenza sugli strumenti che effettivamente servono, in una cornice di pieno rispetto dei principi costituzionali: abbiamo una storia alle spalle che li legittima a tanto!

Mi permetto, a tal proposito, di ricordare, ringraziandola, la Ministra della giustizia francese, Christiane Taubira, che si è dimessa il 27 gennaio scorso. Lo ha fatto

disciplinato tali squadre prima con la Convenzione di Bruxelles del 29 maggio 2000 (art. 13), relativa all'assistenza giudiziaria in materia penale, e quindi con la decisione quadro n. 2002/465/Gai del Consiglio del 13 giugno 2002. Infine, con la raccomandazione del Consiglio dell'8 maggio 2003 è stato adottato anche il modello formale di accordo per la costituzione della squadra di indagine comune, che integra e completa le disposizioni contenute sia nell'articolo 13 della Convenzione, sia nella decisione quadro del Consiglio. Per soddisfare la stessa esigenza di collaborazione, le squadre investigative comuni sono state previste anche dalla *Convenzione delle Nazioni Unite contro il crimine organizzato* transnazionale (art. 19) adottata dall'assemblea generale il 15 novembre 2000 ratificata dalla legge 16 marzo 2006 n. 146.

39 *Schedare i passeggeri è contro i Trattati Ue. Il garante europeo boccia la stretta sui voli*, *La Repubblica*, 10 dicembre 2015.

dichiarando di non poter condividere la spinta del Governo di cui faceva parte verso la costituzionalizzazione dell'emergenza. In questo momento, la *ex* Ministra Taubira incarna la necessità di rispettare le regole della democrazia anche nel contrasto dei più gravi fenomeni socio-criminali e nei momenti in cui essi generano tragedie di proporzioni inimmaginabili.

È la vera cooperazione internazionale che va rafforzata, quella che nulla ha a che fare con la tanto decantata raccolta di milioni di dati che evoca un preoccupante futuro di *"big data"* e che, esattamente come *renditions,* torture e prigioni illegali, rischia solo di fornire ai terroristi storie ed immagini da usare a scopi di proselitismo: così è avvenuto con quella delle tute arancioni indossate dai prigionieri di Guantanamo, immagine sfruttata per la tragica scenografia dei crudeli "sgozzamenti" che, sullo sfondo di un deserto sconfinato, i criminali dell'Isis hanno fatto conoscere al mondo attraverso la diffusione sul web dei relativi filmati.

Tra l'altro, sempre in tema di cooperazione, va aggiunto che sono proprio le convenzioni internazionali che impongono lo scambio spontaneo, immediato e completo delle informazioni[40]!

Purtroppo, però, non è così che, nella realtà, funzionano le cose e potrei citare molti esempi, dalla scarsa e tardiva collaborazione di Belgio e Francia dopo la strage di Parigi del 7 gennaio 2015 nella sede del periodico *Charlie Hebdo*, allorché, nella regione di Chambery, presso il valico del Frejus, il 16.1.2015, le autorità locali fermarono – su richiesta della polizia belga – due fratelli di origina magrebina collegati ad una cellula "disarticolata" il giorno precedente a Verviers (Belgio) mentre stava introducendosi in Italia, alle difficoltà di poter utilizzare nei nostri processi le intercettazioni telefoniche effettuate in Gran Bretagna, per non dire dei problemi in tema di estradizione ed esecuzione di mandati d'arresto europei. Difficoltà che continuano a manifestarsi sin dagli "anni di piombo" e che la magistratura ha denunciato da tempo[41].

---

40 .Lo scambio spontaneo di informazioni, in particolare, è contemplato da alcune Convenzioni, tra cui quella di Strasburgo dell'8.11.1990 sul riciclaggio, quella di Bruxelles del 29.5.2000, tra gli Stati membri dell'Unione europea, in tema di assistenza giudiziaria e quella sottoscritta nel corso dell'Assemblea di Palermo (12-15 dicembre 2000) sul crimine organizzato transnazionale.

41 Sia permesso di citare la relazione di A. Spataro nel Corso di Aggiornamento professionale del Csm sul tema *Terrorismo e crimine transnazionale: aspetti giuridici e premesse socio organizzative del fenomeno*, Roma 5-7 marzo 2007.

11. L'obiettivo della Procura europea antiterrorismo

Nell'ottica della sinergia virtuosa di tutte le forze che possiamo mettere in campo contro il terrorismo e nella prospettiva di futuri sviluppi della cooperazione internazionale, non vi può essere dubbio sul fatto che la istituzione di una Procura europea (Eppo), oggetto di proposta formulata il 17 luglio 2013 dalla Commissione europea[42], costituirebbe un grande passo avanti. Per di più, estendendo gradualmente le sue competenze fino ad occuparsi anche dei reati di terrorismo internazionale[43], l'azione della Procura europea apparirebbe coerente con la natura transnazionale del tipo di criminalità. La prospettiva, allo stato, non può certo considerarsi realistica, poiché è evidente che ciò comporterebbe il passaggio dai Governi alla Procura stessa della guida della strategia investigativa antiterrorismo, ma è certo che, al di là delle citate diversità ordinamentali, la sua azione potrebbe determinare una progressiva omogeneità d'intervento a livello europeo, nelle prassi prima e nelle leggi dopo, persino rispetto al sistema di *common law* inglese, così diverso rispetto al nostro ed a quelli dei Paesi continentali. Ma dubito davvero che ciò possa avvenire a breve, specie ove si consideri – per quel che se ne sa – il contenuto ancora non chiaramente definito della prossima Direttiva del Parlamento europeo e del Consiglio dell'Unione europea sulla lotta contro il terrorismo che sostituirà la Decisione quadro del Consiglio 2002/475/Gai sullo stesso argomento (un testo che suscita preoccupazione per la deriva securitaria da cui è caratterizzato e che rischia di essere approvato in fretta e furia dal Parlamento europeo nel corso dei prossimi mesi senza un vero dibattito sulla sua compatibilità con la Carta).

12. La risposta giudiziaria o di *intelligence* non basta: serve il confronto ed il reciproco rispetto con il mondo islamico

Le affermazioni che precedono potrebbero far nascere il sospetto che chi scrive attribuisca all'azione della magistratura e delle collegate forze di polizia giudiziaria ruoli

42 Trattasi della proposta di regolamento Com(2013)534 – ai sensi dell'art. 86 Tfue (Trattato sul funzionamento dell'Unione europea, introdotto dal Trattato di Lisbona).

43 Per un'articolata riflessione sul punto, si veda *Procura europea e reati di terrorismo: un connubio impossibile?* di Andrea Venegoni, magistrato addetto all'Ufficio del ruolo e del massimario della Corte di cassazione, in *Questione Giustizia online*, del febbraio 2015, www.questionegiustizia.it/articolo/procura-europea-e-reati-di-terrorismo_un-connubio-impossibile__12-02-2015.php.

e competenze da sé sufficienti a sconfiggere questo terrorismo. Non è così, poiché nessuno può seriamente pensare che il successo sperato possa essere raggiunto solo con le indagini, con i processi o con la cosiddetta attività di *intelligence*, e neppure con la guerra. Occorre all'evidenza anche la piena e convinta collaborazione delle comunità da cui i terroristi spesso provengono. Sarebbe facile, a tal proposito, invocare la necessità di favorire la integrazione delle comunità degli immigrati nel nostro tessuto sociale, ma occorre anche altro, qualcosa di diverso e di più specifico. Il processo di integrazione richiede spesso un lungo cammino, ma è pur vero che nelle nostre democrazie è ben praticabile la strada del confronto con i musulmani, attraverso la rottura della incomunicabilità e per stabilire le basi di un rispetto reciproco. Il vero universalismo dei diritti, come è stato scritto, sta proprio in questo, nel rispetto – ovunque – delle persone come sono, evitando ogni tendenza a trasferire su tutti i componenti di una comunità le responsabilità di pochi o di una parte della medesima, così costruendo muri insormontabili.

Conforta, a tal proposito, che, con il decreto legge n. 7 del 2015, il Governo abbia respinto ogni indegna pulsione xenofoba, come quella che strumentalmente ha portato qualcuno ad assimilare al rischio-terrorismo il dramma di tanti immigrati, anche irregolari, che approdano sulle coste dell'Europa meridionale accompagnati dalla sola speranza di trovare condizioni di vita dignitose.

Ma devono anche essere abbandonate tattiche irragionevoli per assecondare impresentabili umori (da ogni fronte politico si concorda, ad es., sulla inutilità del reato di immigrazione clandestina, che danneggia pure le indagini, ma si preferisce rinviarne la abolizione perché «non è il momento»), così come va evitata la prassi degli "annunci" mediatici, che vedono alternarsi quelli sulle "rassicuranti" espulsioni di persone sospette alle celebrazioni dei successi delle nostre forze di *intelligence*, le notizie sui progetti di attentato sventati e quelle sugli elevati numeri dei *foreign fighters* identificati: una successione di messaggi che fa crescere le paure collettive e spinge a temere persino il vicino. Come dimenticare l'annuncio relativo all'arresto – peraltro richiesto dalle autorità tunisine – di un giovane marocchino, Abdelmajid Touil, presentato con enfasi come corresponsabile dell'attentato al Museo del Bardo di Tunisi del 18 marzo 2015? Dopo circa sei mesi di carcere, è stato alla fine scarcerato e, pur andando incontro al rischio della pena di morte, sarebbe stato espulso come era stato subito annunciato, se la Procura di Torino e quella di Milano non fossero intervenute, nell'ambito delle loro rispettive competenze, per impedirlo. Solo nel febbraio 2016 il giovane è uscito dall'incubo: gli è stato infatti consegnato il permesso di soggiorno temporaneo, in attesa dell'asilo politico.

È da accogliersi con favore, allora, il diffondersi della fiducia nella interlocuzione con le comunità islamiche che – al di là delle iniziative preannunciate dal Governo – deve avvenire non solo coinvolgendone i rappresentanti istituzionali, ma anche attraverso scuole, formatori, network e ogni possibile canale di informazione in grado di vincere la fatale attrazione che le "tecniche" dell'IS potrebbe esercitare su giovani sprovveduti.

Non abbiamo la speranza di vincere presto contro questo terrorismo ma perché ciò avvenga nel minor tempo possibile occorre che vi sia massima attenzione e rispetto per le identità degli altri che non possono e non devono annullarsi. Mi permetto di citare, come esempio virtuoso di ciò che occorre, la bella iniziativa che è stata presa dalla Camera dei deputati, il 19 gennaio scorso, dalla Presidente Laura Boldrini che ha organizzato e presieduto un incontro intitolato: «Le donne contro Daesh: il contrasto al radicalismo ed al fondamentalismo». Certo, iniziative come queste non esauriscono quello che si può fare, specie in un contesto di sfida complicatissima da ogni punto di vista, ma sono decisamente importanti nella direzione del confronto e del reciproco rispetto e per far comprendere che l'Europa non può affatto trasformarsi in una fortezza assediata, che sicurezza e libertà sono ben conciliabili e che cultura e democrazia sono fattori unificanti ed irrinunciabili.