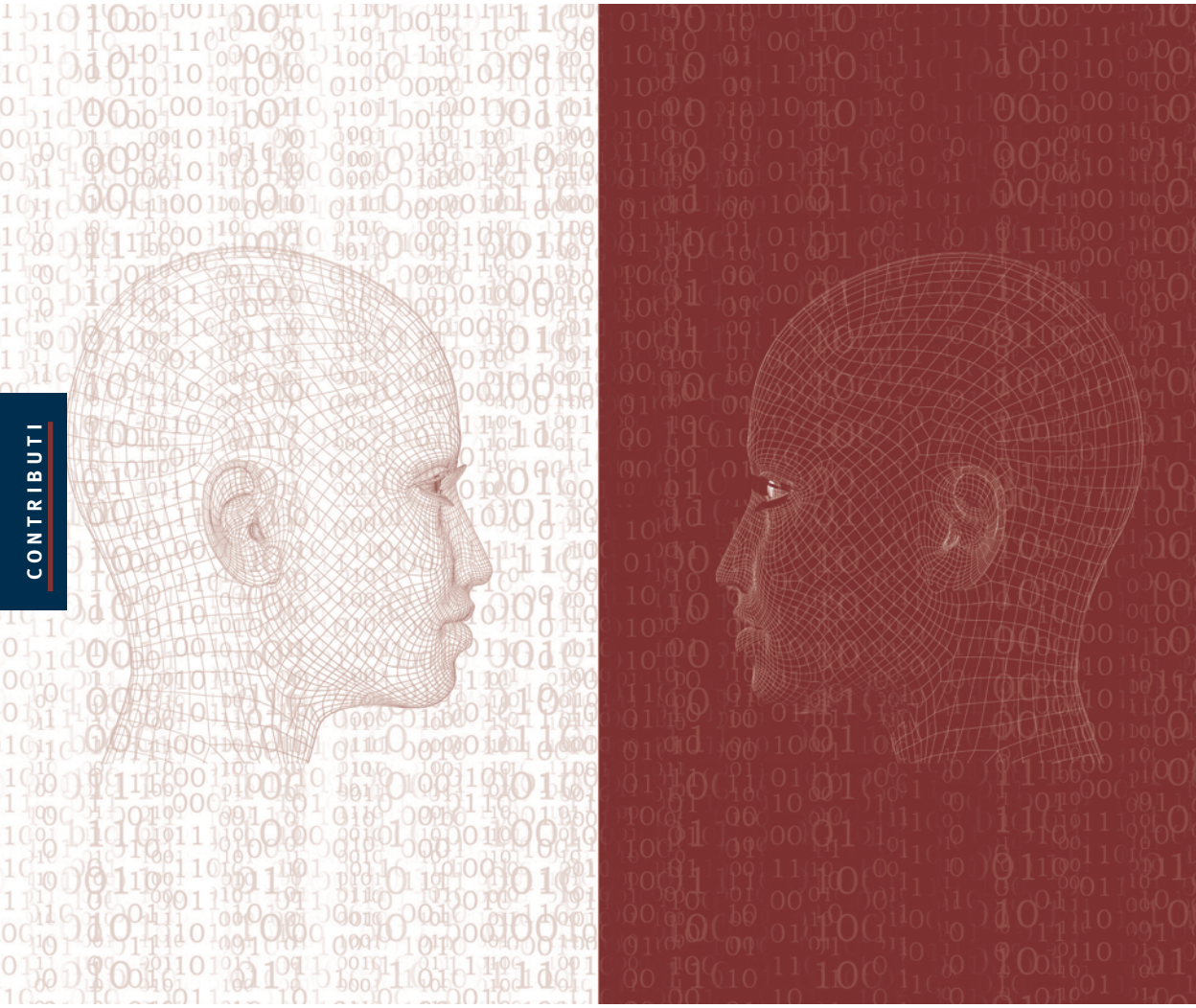
La società sorvegliata
I nuovi confini della libertà

CONTRIBUTI



Atti del Convegno - 28 gennaio 2016

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Antonello Soro, *Presidente*
Augusta Iannini, *Vice Presidente*
Giovanna Bianchi Clerici, *Componente*
Licia Califano, *Componente*

Giuseppe Busia, *Segretario generale*

Piazza di Monte Citorio, 121
00186 Roma
www.garanteprivacy.it

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

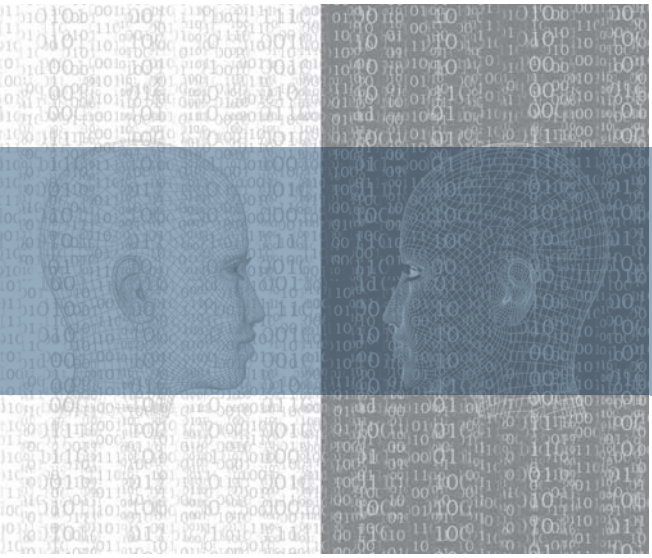
La società sorvegliata
I nuovi confini della libertà

Atti del Convegno
28 gennaio 2016

www.garanteprivacy.it

In questo volume sono raccolti i contributi di studiosi ed esperti intervenuti al Convegno "*La società sorvegliata. I nuovi confini della libertà"*, organizzato dal Garante per la protezione dei dati personali in occasione della "Giornata europea della protezione dei dati personali" 2016.

Indice



La società sorvegliata
I nuovi confini della libertà

Apertura dei lavori

Antonello Soro
Presidente del Garante
per la protezione dei dati personali

Apertura dei lavori

La società sorvegliata
I nuovi confini della libertà

Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali

Era il lontano 1787 quando Jeremy Bentham ideò il Panopticon, l'architettura di un carcere ideale, nel quale i detenuti sanno di poter essere costantemente osservati, ma non possono verificare se il controllo davvero si verifica.

Sono dunque visti ma non vedono, sono oggetto di un'informazione ma non soggetti di una comunicazione.

Due secoli dopo Michel Foucault spiegherà come il potere disciplinare si eserciti rendendosi invisibile e, ad un tempo, imponendo ai sorvegliati la totale trasparenza, la visibilità obbligatoria e costante.

L'esercizio del potere diviene così, nel sorvegliato, coscienza inquieta della propria visibilità. Che è, essa stessa, limitazione della libertà.

Forse non esiste metafora più opportuna del Panopticon per descrivere il rapporto tra ciascuno di noi e le infinite forme di sorveglianza cui siamo, a volte anche volontariamente, soggetti e che, astraendo, possiamo ricondurre al potere pubblico e a quello dei privati.

A questa dicotomia rimandano anche le due sentenze della Corte di Strasburgo (una sui controlli datoriali sul lavoratore, l'altra sulle intercettazioni da parte dei Servizi) depositate lo stesso 12 gennaio di quest'anno, quasi a tratteggiare i "nuovi confini della libertà".

Libertà sempre più insidiata da forme di controllo sottili, pervasive e capaci per questo di annullare - se non adeguatamente

regolate - ogni possibilità per l'individuo di "costruirsi liberamente" (secondo una delle più belle definizioni della privacy).

Il progresso della tecnologia - con una molteplicità di strumenti sempre più sofisticati e interconnessi - ha reso possibile un continuo processo di raccolta dei nostri dati, agevolmente archiviati a costi contenuti, ampliando a dismisura lo spettro delle attività che possono essere svolte da chi quei dati conserva e analizza.

L'economia digitale si avvale di strumenti di controllo inseriti nei dispositivi d'uso quotidiano, la cui facilità di utilizzo contrasta con la pervasività e, soprattutto, con regole trasparenti che rendano pienamente edotti gli utenti dell'uso - e delle finalità - che quei dati consentiranno di realizzare.

A questa tecnologia sempre più invasiva si affiancano "controllori" invisibili, processi di elaborazione e cessione di dati a terzi, spesso frammentati tra una moltitudine di soggetti in un contesto globalizzato, nonché la possibilità di conservare i dati per tempi illimitati.

Si delinea quindi un sistema di sorveglianza capillare che noi stessi, più o meno consapevolmente, alimentiamo, per l'incontenibile desiderio di condividere tutto ciò che ci riguarda.

Ma esiste un rovescio della medaglia.

La "florida" economia dei dati, che offre straordinarie opportunità di sviluppo, ha la potenzialità concreta di trasformare la persona profilata in docile oggetto di poteri altrui.

Per altro verso è evidente quanto sia difficile essere "tecnologicamente" soli in ambienti sempre più intelligenti e connessi.

Nell'esperienza quotidiana siamo bersagliati - con un misto di nostra meraviglia e ammirazione - da nuovi servizi e nuove applicazioni e poiché nella dimensione digitale l'integrità fisica è rispettata, la percezione dei rischi per le nostre persone è praticamente inesistente.

Ma quando l'algoritmo diviene la chiave attraverso la quale scelte e comportamenti vengono orientati, non possiamo non

chiederci seriamente a quanta libertà siamo disposti a rinunciare pur di continuare a sfruttare tutti i benefici offerti dalle tecnologie.

Le stesse potenzialità dei Big Data, anche rispetto a dati anonimi o aggregati, lasciano intravedere rischi di nuove forme di discriminazione per effetto di analisi sempre più puntuali e tecniche di re-identificazione sempre più raffinate.

Il rischio della facile accessibilità ai dati e della loro condivisione è quello di un loro utilizzo per molteplici e differenti funzioni e interessi, indistintamente da parte di soggetti pubblici o privati.

Penso a quello che potrebbe accadere - o forse accade - nel campo delle assicurazioni, della salute, del lavoro.

Sono convinto che dovremmo contrastare la deriva per cui la persona è considerata come una "miniera a cielo aperto" da cui attingere liberamente, per elaborare profili - individuali, familiari, di gruppo - funzionali ai bisogni di una società compressa tra le esigenze di sicurezza, incalzata dagli interessi dei produttori di tecnologie, minacciata da sottili strategie di esclusione.

È anche per questo che la privacy come libertà dal controllo è condizione della democrazia e del pluralismo, presupposto di dignità e garanzia contro ogni discriminazione.

E garanzie ancor più stringenti devono essere previste rispetto al potere investigativo, tanto più in un tempo in cui la minaccia del terrorismo del *"tempo ordinario"* rischia di diventare un dato strutturale della nostra quotidianità.

Certo, di fronte a chi usa le stragi quale strumento di affermazione e reclutamento, unendo capacità simmetrica (militare) e asimmetrica (attentati), diventa forte la tentazione di scorciatoie emergenziali.

Penso al paradosso della Francia che vuole inserire l'emergenza in Costituzione.

Ma questo vorrebbe dire non solo tradire la nostra stessa identità democratica ma anche fare il gioco dei terroristi, che puntano alla negazione dei principi su cui si fondano le democrazie occidentali.

Ha ragione Alain Touraine, quando afferma che per battere l'IS dobbiamo essere "più efficaci, non meno liberi".

Il Parlamento europeo con la Risoluzione del 25 novembre ha invocato una strategia di contrasto del terrorismo tanto rigorosa quanto capace di mettere al centro i diritti e le libertà.

Soprattutto perché non tutte le limitazioni della libertà sono efficaci davvero per renderci più sicuri.

Si potrebbe citare, per tutti, l'esperienza delle Agenzie americane, con la raccolta generalizzata e indiscriminata di informazioni sulla vita di tutti i cittadini, così numerose da essere poi inutili perché ingestibili.

La stessa strage del Bataclan parrebbe essere stata realizzata da soggetti tutt'altro che ignoti agli organi inquirenti: dunque ciò che è mancato sembra essere non tanto le informazioni quanto una loro raccolta più efficace perché più selettiva e, dunque, un'analisi capace di cogliere sviluppi e tendenze di rischi già probabilmente evidenti.

Anche il PNR - uno degli elementi su cui si fonda la strategia europea di contrasto del terrorismo - potrà essere efficace solo nella misura in cui di tutta quella massa di dati raccolti si faccia un utilizzo, appunto, ragionevole, selettivo e mirato in ragione dei fattori di rischio emersi nei riguardi di determinati soggetti.

Il rischio della delega delle indagini ad algoritmi e selettori più o meno ampi è, infatti, proprio quello di sottovalutare l'importanza del fattore umano, capace esso solo di dare senso e forma a masse di dati, altrimenti prive di alcun significato.

L'efficacia della strategia difensiva mi sembrerebbe presupporre, allora, il suo rivolgersi non alla generalità dei cittadini ma a "bersagli" e canali rivelatasi maggiormente pericolosi, a seguito di indagini che non possono che fondarsi su tecniche di sorveglianza mirata.

Se alcune di queste tecniche sembrano ineliminabili (come faranno probabilmente parte del nostro arredo urbano, di qui al futuro, telecamere intelligenti e sistemi integrati di sicurezza

urbana), penso che debbano essere comunque utilizzate nella maniera più utile in termini di prevenzione e più sostenibile sotto il profilo democratico.

Il che vuol dire rendere le analisi il più possibile selettive e rafforzarne il sistema di garanzie.

Che si articola in previsioni legislative tassative capaci di limitare l'ammissibilità di tali strumenti investigativi ai soli casi realmente indispensabili per la tutela di interessi fondamentali, con uno standard minimo di concretezza dei sospetti necessari per giustificare il ricorso a tali misure (così valutando anche l'ampiezza dei "selettori"e la "catena dei contatti" cui si possano estendere le captazioni).

E di qui anche l'importanza del triplice controllo parlamentare, giudiziale e "tecnico", tale da impedire che l'intelligence strategica degeneri in sorveglianza massiva.

È figlia di questa sensibilità la sentenza del Tribunale costituzionale che ha dichiarato illegittima la legge portoghese sui Servizi, ove non prevede un vaglio giurisdizionale intrinseco, analogo a quello del processo penale, sulla richiesta di acquisizione dei tabulati.

E lo è anche la recentissima sentenza della Corte europea dei diritti umani, sull'illegittimità delle intercettazioni preventive svolte dai Servizi ungheresi in assenza di autorizzazione giudiziale e di un limite temporale definito, nonché di alcuna procedura che, una volta cessate le esigenze di prevenzione, renda edotto l'interessato di essere stato sottoposto a controllo.

E mira a impedire la sorveglianza totale (ancorché del singolo indagato) anche la sentenza del 26 giugno della nostra Cassazione.

Essa ha, infatti, dichiarato illegittima la realizzazione di intercettazioni ambientali mediante immissione, nel telefono dell'indagato, di un virus capace di attivare la videocamera in qualsiasi momento, senza alcuna delle limitazioni previste dal codice, a tutela di quella sfera ineliminabile di riservatezza

che l'art. 15 della Costituzione accorda a chiunque, qualunque sia la sua posizione processuale.

Se poi consideriamo che in Italia questo tipo di intercettazioni da remoto sono state realizzate attraverso un sistema (Galileo) venduto da una ditta privata che in estate ha subito un attacco, disperdendo in rete una quantità immensa di dati anche riservati per ragioni investigative, comprendiamo come nessun'azione di difesa dal terrorismo possa prescindere da un'adeguata strategia di sicurezza cibernetica, che protegga i dati, i sistemi che li ospitano e le infrastrutture su cui viaggiano le comunicazioni.

In questo senso, allora, la protezione dei dati personali è essa stessa essenziale presupposto non solo della cyber security ma, più in generale della sicurezza pubblica.

Se, infatti, le banche dati strategiche su cui si fonda l'intero sistema della sicurezza pubblica e della prevenzione non sono adeguatamente protette, sono le nostre democrazie a divenire vulnerabili proprio di fronte a un terrorismo che sempre più usa la rete per fare proselitismo.

Ed è proprio un'adeguata protezione dei dati personali (ancorché solo dei cittadini americani!) una delle componenti essenziali della riforma voluta da Obama, entrata in vigore meno di due mesi fa negli Usa e che si avvicina al modello europeo di prevenzione, proprio nel momento in cui invece è l'Europa a rischiare di allontanarsi da se stessa e dalla sua identità profonda.

È anche per questo, per preservare la nostra autentica identità (che non è certo etnica ma culturale e valoriale) che la reazione alla minaccia terroristica deve saper essere efficace ma rispettosa dei diritti e delle libertà fondamentali.

Di questo parleremo oggi, di come le varie forme di sorveglianza, più o meno occulte o pervasive, di fonte pubblica o privata, stiano ridefinendo la percezione e, forse, la stessa ragione del nostro essere persona.

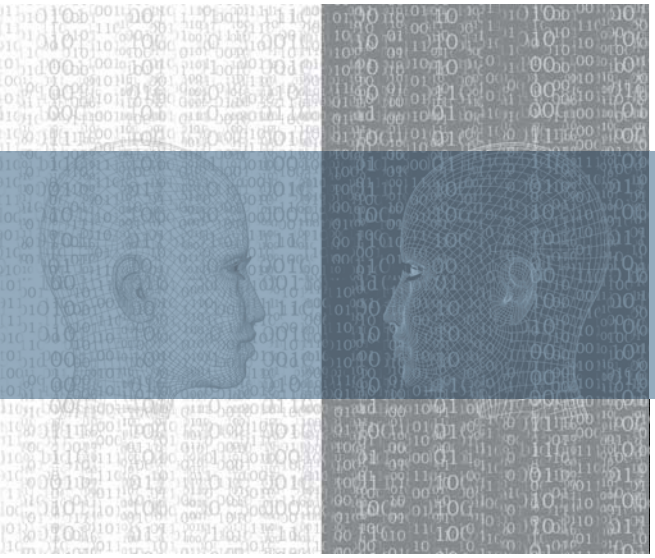
In gioco vi sono i limiti che la "libertà e la dignità umana"

impongono all'iniziativa economica privata (art. 41 Cost.) e il senso stesso che attribuiamo al rapporto tra individuo e mercato.

Ma vi è anche l'idea della democrazia in cui vogliamo riconoscerci, in quel difficile e sempre mutevole equilibrio tra libertà e sicurezza, che misura il grado di civiltà di un Paese.

Proprio perché spazieremo su questi temi e su questi orizzonti, con un approccio che non può non arricchirsi di sensibilità diverse, ascolteremo magistrati, esponenti del Governo, avvocati, filosofi, giornalisti, sociologi.

Quanti, cioè, analizzano ogni giorno, vivono e spesso anche determinano i grandi cambiamenti che ridefiniscono, oggi, i confini della nostra libertà.



Quanto controllo può sopportare una democrazia?

Sessione I

Giuseppe Roma
Sociologo

Armando Spataro
Magistrato

Marco Minniti
Sottosegretario alla Presidenza del Consiglio dei Ministri

Moderatore **Augusta Iannini**
Vice Presidente del Garante per la protezione dei dati personali

Sessione I

Quanto controllo può sopportare una democrazia?

Augusta Iannini

Buongiorno, grazie ai relatori per essere intervenuti a questa nostra Giornata europea della protezione dei dati personali. La prima sessione ha come titolo: *"Quanto controllo può sopportare una democrazia?"*. Il Presidente Soro ha già introdotto tutti i temi di questo dibattito, io mi limiterò invece a riferire alcune esperienze più o meno concrete. Parto da un'osservazione storica: già nel 1500 Shakespeare, nel suo Enrico V, ammoniva che il re prende nota di tutte le intenzioni dei suoi sudditi con mezzi che nemmeno si possono immaginare. Eravamo nel 1500, ma nel 1985 un sociologo americano che si chiama Gary Marks, affermava che grazie alla tecnologia informatica sta crollando una delle ultime barriere che ci separano dal controllo totale. Io direi che evidentemente la sorveglianza contemporanea è più invasiva di quella di Enrico V, perché non solo lo Stato ma anche le aziende commerciali, le agenzie e le organizzazioni raccolgono tantissimi dati personali.

Conosciamo quel è il loro scopo, che è quello di profilare in maniera sempre più mirata, ma con una differenza per i privati e per il pubblico, perché il privato utilizza, o almeno dovrebbe utilizzare, un consenso più o meno consapevole, mentre nel controllo pubblico questo non avviene. In tal modo nel nome della sicurezza pubblica si registra l'unico matrimonio che oggi definirei ancora indissolubile, perché i dati raccolti a fini commerciali, quelli tratti dalla navigazione su Internet, le immagini raccolte dalla videosorveglianza, gli sfoghi che ognuno di noi posta sui

social network in maniera più o meno avveduta, sono utilizzati insieme ai dati raccolti per finalità di sicurezza pubblica, e/o di prevenzione e repressione dei reati.

In questo modo si rischia di definire prima il profilo del possibile colpevole e magari poi, con l'aiuto di un algoritmo, gli si modellano addosso gli indizi e le prove. Per altre finalità, per esempio, le società private progettano di disegnare valutazioni reputazionali utilizzando processi matematici. Il *rating* reputazionale sarà determinato attraverso la valorizzazione numerica, in positivo o in negativo, di fatti con rilevanza giuridica economica e sociale, che sono contenuti in documenti certamente di verificata genuinità, ma grondanti di dati personali di soggetti che partecipano a pagamento a questa community, dove si decide la loro reputazione. Credo che questo ci debba far pensare, soprattutto per l'aspetto della partecipazione a pagamento.

In Cina si stanno addirittura sperimentando dei nuovi sistemi di valutazione del rischio e della solvibilità degli utenti, al fine di concedere o meno dei prestiti e questi criteri di valutazione si fondano anche sui Big Data on-line, cioè sui dati relativi alla navigazione on-line e alle altre esperienze in rete dei singoli cittadini. La prospettiva però non è soltanto quella della valutazione commerciale, ma sarebbe quella di creare un vero e proprio database, dal quale il Governo possa attingere per esprimere valutazioni di ampio raggio sui cittadini, sulla loro onestà, sulla loro moralità. In questo modo si introdurrebbe una specie di "rating" che si ripercuote poi anche sull'accesso ai servizi sanitari, all'istruzione, al mondo del lavoro. Si creerebbe inoltre quello che una attenta giornalista, Patrizia Licata, sul Corriere della comunicazione di qualche giorno fa, ha definito un micidiale cocktail fatto di alta tecnologia, aziende guidate dal profitto, politica autoritaria e scarse libertà civili.

Siamo proprio sicuri che nel libero e democratico Occidente non stia avvenendo la stessa inquietante profilazione? Tutto questo è ancora compatibile con il concetto di democrazia, cioè con il

principio che le autorità non hanno poteri illimitati, che ci sono pesi e contrappesi, che nessuno è al di sopra della legge e che tutti devono rispondere di quello che fanno? In una società così controllata è ancora possibile parlare di democrazia? Arrivo dunque al tema del dibattito: come cambia il rapporto tra democrazia e controllo globale, quando la finalità è quella della sicurezza?

Il Vice Presidente di Google, in una intervista del 2013, sembra disegnare una via, perché riflette e conclude: uno Stato in cui la privacy è totalmente rispettata, è uno Stato insicuro. Uno Stato in cui, al contrario, chi governa sa tutto dei propri cittadini, è il massimo della sicurezza. Io credo che nessuno voglia vivere in questi due estremi e quindi dobbiamo trovare un punto di equilibrio tra privacy e sicurezza.

Allora penso che bisogna fissare delle regole, ma queste regole devono limitarsi a disciplinare le utilizzazioni consentite?

Oppure devono imporre delle vere e proprie limitazioni alla raccolta dei dati?

Questo è l'interrogativo che io vorrei proporre ai partecipanti a questa tavola rotonda. Nella ricerca di un equilibrio, a che condizioni i piatti della bilancia pesano in eguale misura la sicurezza da un lato e la riservatezza dall'altro? La coesistenza di tutti gli interessi si realizza meglio consentendo l'acquisizione indiscriminata dei dati e limitandone l'utilizzazione, o intervenendo, invece, all'origine, limitando l'acquisizione dei dati?

A questa e ad altre domande spero potranno rispondere i relatori che mi appresto ad introdurre. C'è un'inversione dell'ordine degli interventi, parlerà per primo il dottor Giuseppe Roma, già Direttore del Censis per molti anni. Si è occupato spesso di questi temi, ha presentato uno studio sul valore della privacy nell'epoca della personalizzazione dei media. Io credo che potrà rispondere a tutti questi interrogativi, anche attraverso l'analisi della percezione che gli individui hanno rispetto alle tematiche della sicurezza e della tutela dei dati personali.

Prego.

Giuseppe Roma

Il tema della mia relazione è stato ben delineato dal Presidente Soro, e riguarda il rapporto che c'è fra democrazia, rischi, sicurezza e controllo. Inizierei esattamente da questo principio: ci sentiamo oggi molto più esposti a rischi di natura diversa, il terrorismo certamente ma anche l'inquinamento, la perdita del lavoro, le turbolenze finanziarie che rendono vulnerabile il nostro risparmio, la criminalità diffusa che è un vecchio portato delle paure più vicine a noi, nel nostro quartiere, nelle nostre città.

Il primo tema: la democrazia. Oggi sappiamo come la democrazia sia soggetta a diverse modificazioni, ma vorrei dare un giudizio molto secco in proposito: non credo che la democrazia sia a rischio se il controllo e gli strumenti di prevenzione si basano su due saldi princìpi di lealtà istituzionale. Il primo è che la politica non sfrutti la paura. Purtroppo, tuttavia, sappiamo che questo a volte succede, sappiamo come le paure costituiscano la base stessa per avere consenso, e, con esso, poter eccedere nel controllo.

Il secondo riferimento è che le politiche di sicurezza e di prevenzione, abbiano uno stretto collegamento con la dimensione sociale, quindi con la possibilità che le persone non si sentano isolate e non siano estranee alle relazioni sociali.

Viviamo e veniamo da un periodo di fortissimo soggettivismo personale, in cui l'individuo ha pensato di non avere alcun limite. Un libro di Remo Bodei uscito di recente tratta proprio il tema del "limite". Abbiamo continuamente spostato in avanti i limiti, ritenuti in precedenza da non superare, nelle scienze, nella biologia, persino nell'etica e nella morale.

Spostare continuamente i limiti e quindi allargare la sfera di libertà soggettive, presenta oggi alcune patenti contraddizione: non vale per tutti. Basti pensare alla difesa da parte di alcune comunità nazionali dai flussi migratori, dove vengono posti addirittura limiti fisici, vere barriere di protezione. Ma c'è un atteggiamento ancora più contraddittorio che sta dentro il soggetto, riguarda la persona.

Come è emerso con chiarezza in una ricerca che realizzai proprio per l'Autorità, da una parte vogliamo limitare l'accesso alle informazioni che ci riguardano, richiediamo giustamente protezione dei nostri dati personali ma, nello stesso tempo, siamo noi stessi la principale fonte informativa sulla nostra vita, esibendo on line le nostre immagini, i nostri pensieri, il nostro modo di essere.

In un tale ambiguo insieme di comportamenti sociali va inquadrato il rapporto fra democrazia e sicurezza.

I più recenti attacchi terroristici hanno messo alla prova gli apparati di sicurezza incentivando interventi operativi e, in taluni casi, anche legislativi (come in Francia), volti a migliorare la tenuta del sistema.

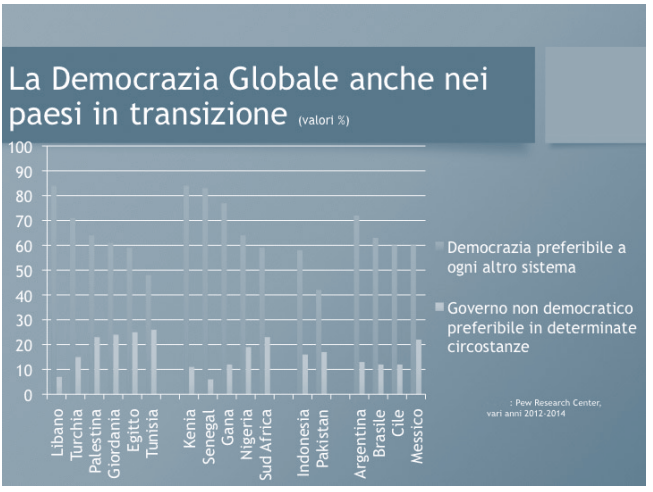
Maggiore controllo del territorio, più potere alle forze di polizia, raccolta massiva di comunicazioni e dati personali, sono conseguenze dirette di un tale stato d'allerta, che interessa buona parte dei paesi europei. Intervenire su libertà e diritti implica, naturalmente, una valutazione del necessario equilibrio fra tutela ed esercizio della democrazia.

Tale problematica s'innesta, poi, sul più generale dibattito riguardante le recenti trasformazioni dei principi storici e delle prerogative funzionali dei regimi democratici, determinate dalla globalizzazione dell'economia e dalle tecnologie della comunicazione.

La democrazia si presenta, oggi, come modello istituzionale più

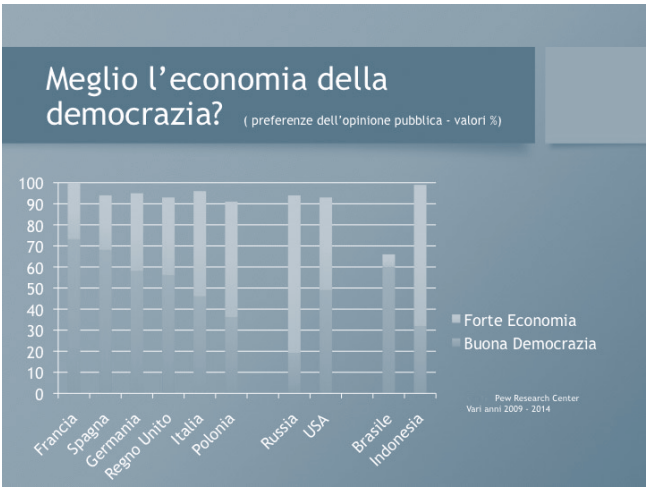
"resiliente", flessibile e adattivo, ma non necessariamente più efficace. Inoltre, proprio la prepotente affermazione della rete sta minando, nei fatti, i principi della democrazia rappresentativa, assottigliando la separazione fra la "sovranità popolare" (che legittima il potere politico) e i "rappresentanti" (che lo esercitano in modo legittimo).

Di fronte alla complessità di questi cambiamenti, metal detector, video sorveglianza, intercettazioni telefoniche e telematiche, etc. vanno utilizzate con estrema cautela, ma non sembra possano rappresentare un pericolo mortale della democrazia. Nel mondo globale, le istituzioni democratiche costituiscono per l'opinione pubblica il sistema di organizzazione sociale preferibile a ogni altro. Tuttavia, in paesi in transizione (come Egitto, Tunisia, Sud Africa o Messico) una quota significativa dell'opinione pubblica (compresa fra 20-25%) propende verso regimi autoritari per affrontare situazioni particolari.



Nel contempo però anche nelle nostre democrazie, quelle che difendono fortemente i principi generali, c'è un'altra questione: il rapporto fra la democrazia e l'economia. Nei paesi di più consolidata democrazia il confronto fra politica ed economia non evidenzia un primato della prima sulla seconda. Solo in Francia, Germania, Spagna e Regno Unito la maggioranza dei cittadini preferisce una democrazia funzionante a una forte economia; in Italia e negli Stati Uniti l'opinione pubblica è divisa a metà, mentre

Paesi come Polonia, Russia o Indonesia preferiscono decisamente il benessere economico.

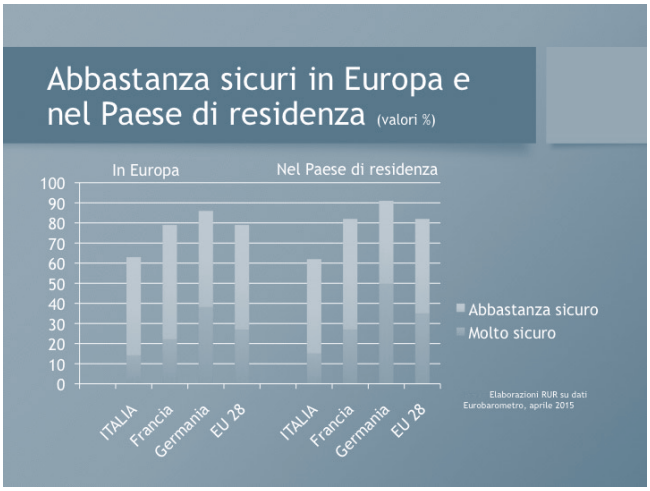


Per dirla con Robert Dahl, esiste una perenne tensione fra democrazia ed economia di mercato. Le disparità di reddito favoriscono massicciamente anche l'ineguale distribuzione delle risorse politiche, tuttavia la democrazia ha nell'economia di mercato una condizione vitale di sopravvivenza, in quanto i meccanismi di mercato inducono nella società pluralismo e merito.

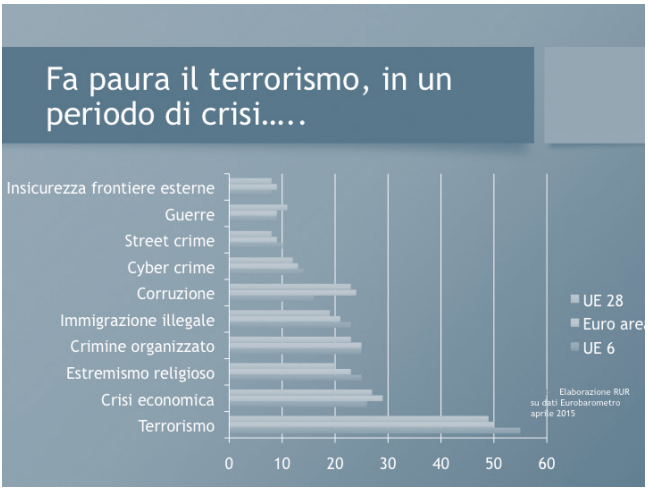
Fattori che non sono, tuttavia, operanti in modo omogeneo nell'economia globale finanziarizzata.

L'Europa resta un territorio ritenuto, dai suoi abitanti, sufficientemente sicuro: per il 27% degli europei è "molto sicuro" e per un ulteriore 52% è "abbastanza sicuro", complessivamente quindi il 79%. Altrettanto vale per il Paese di residenza con il 35% di molto sicuri e il 47% di abbastanza sicuri, per un totale dell'82%.

Per gli italiani il senso di sicurezza si riduce significativamente, in riferimento a tutte le dimensioni territoriali considerate. In particolare, rispetto a un valore medio europeo dell'82% di sufficientemente sicuri all'interno dei confini nazionali, gli italiani calano al 63%; nella propria città il valore medio europeo è dell'89%, in Italia del 76%; nel proprio quartiere di residenza dal 90% della media UE si scende al 79%.



Siamo più impauriti tanto più ampio è il territorio di riferimento, cioè abbiamo più paura in Europa, nel nostro Paese e poi gradatamente, quando arriviamo nel nostro quartiere, ci sentiamo più sicuri, quindi è chiaro che la dimensione percettiva è la dimensione vincente.



Ma quali fenomeni inducono insicurezza per gli europei? Al primo posto fra le motivazioni che inducono insicurezza per i cittadini europei si colloca il terrorismo, subito seguito dalla crisi economica. Nella recente indagine dell' Eurobarometro dell'aprile 2015 per il 49% dei residenti nell'UE il terrorismo rappresenta

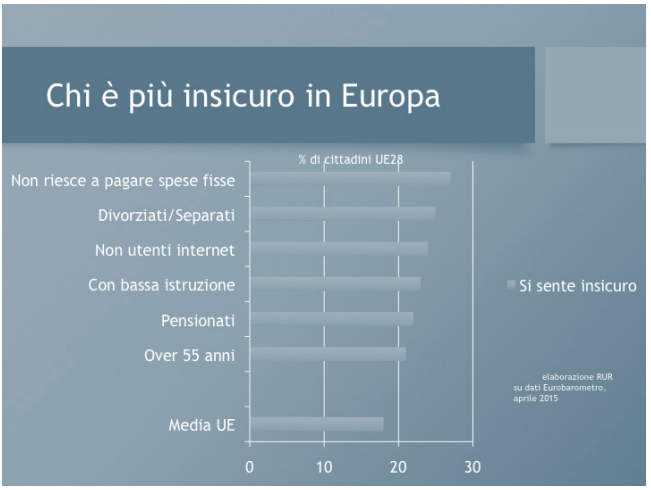
la principale causa delle paure, una quota che sale al 55% nei paesi del nucleo fondatore della UE (Italia,Francia,Germania e Benelux).

In questi Paesi, come nell'intera Unione, la seconda motivazione, tuttavia, è rappresentata dalla crisi economica su cui converge il 26% degli intervistati, poi l'estremismo religioso e la criminalità organizzata per il 25%.

Sulle principali sfide riguardanti la sicurezza gli italiani sono fondamentalmente allineati con i valori europei: bisogna intervenire contro il terrorismo (66%), la criminalità organizzata (54%) e per la sicurezza delle frontiere europee (41%).

Minore sensibilità si rileva rispetto al cyber crime che é ritenuto obiettivo prioritario solo per il 30% degli italiani, ma lo é per il 42% degli europei.

Un dato molto interessante riguarda le caratteristiche di chi è più impaurito in Europa: il valore medio del 18% dei residenti, sale al 27% fra chi è in difficoltà economica non riuscendo a far fronte alle spese fisse, al 25% per divorziati e separati, al 24% per chi non accede a internet, al 23% di chi ha un basso livello d'istruzione, al 22% dei pensionati e al 21% degli over 55 anni.



La *"diseguaglianza della paura"* quindi, esiste visto che si sente più insicuro chi ha più problemi economici, ma soprattutto chi è più isolato e meno informato.

La dimensione che più ci salva dalle paure è la conoscenza, la relazione e quindi la dimensione di rete, che, tuttavia, da una parte realizza nuove modalità di integrazione, ma dall'altra ci profila, si insinua, diventa prepotente. Soprattutto per quanto attiene al marketing commerciale siamo, oggi, soggetti a un'enorme pressione a forme di fastidioso *"inquinamento digitale"*. Se la pubblicità televisiva fu definita strumento dei persuasori occulti, la rete tende a imporre i suoi messaggi e soprattutto a interferire pesantemente nella navigazione sul web. L'utilizzo di dati personali per finalità commerciali non può che differenziarsi fortemente da un uso finalizzato a garantire il bene comune della sicurezza. La *"digital pollution"*, che secondo me sta assumendo proporzioni decisamente eccessive, non deve inquinare l'uso di Internet come fonte di informazione, cioè come aiuto per suscitare consapevolezza, strumento principale per affrontare le paure e le insicurezze.

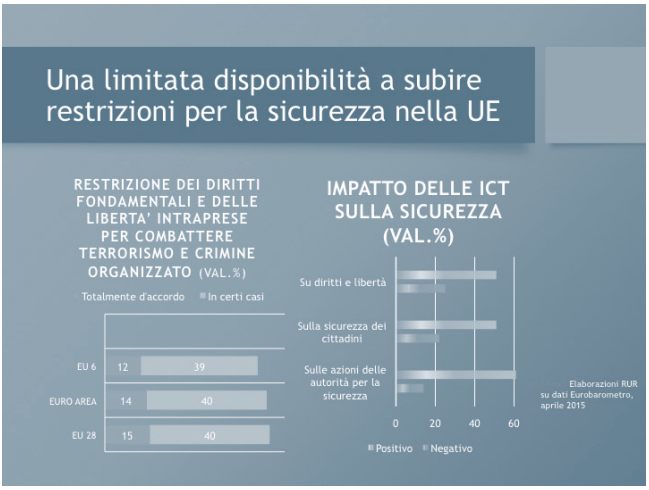
Parlando di che cosa fa paura, al secondo posto c'è la crisi economica, quindi questi due aspetti, il primo più di tipo personale, la percezione del rischio personale, del benessere personale e la percezione del terrorismo sono due cose che dobbiamo considerare anche insieme.

Se guardiamo le dinamiche riguardanti il nostro Paese vedete come con il tempo, (2011-2015) il terrorismo sia passato dal 56 al 66%, un valore eguale alla media europea, ovvero il 65%.

La criminalità organizzata è cresciuta ma non tantissimo. La cosa che a me sembra abbastanza difforme dalla percezione che tutti noi abbiamo è che la criminalità in rete, come sfida di sicurezza, in Italia è diminuita, è anche più bassa della media europea, passa dal 39 al 30% mentre la media europea è il 42%. Questo può collegarsi con il fatto che gli italiani hanno meno esperienza della rete, che ci sia ancora un *digital divide* molto ampio.

Cresce invece la preoccupazione per quello che succede alle frontiere dell'Europa, e pertanto le quattro sfide di sicurezza che ci consegnano gli italiani e gli europei sono: terrorismo, criminalità organizzata, cyber crime e frontiere.

Dentro questo quadro siamo tutto sommato in una democrazia forte, il sistema che meglio può affrontare le tematiche della sicurezza e della garanzia dei propri dati personali, si vede abbastanza precisamente solo una minoranza degli europei consideri la restrizione dei diritti fondamentali e delle libertà come una cosa da praticare in ogni caso, siamo al 15%. Se aggiungiamo il 40% che dice "in limitati casi" vediamo che metà della popolazione europea rifiuta qualsiasi forma di limitazione. Una società iper soggettiva è anche una società che non vuole limiti.



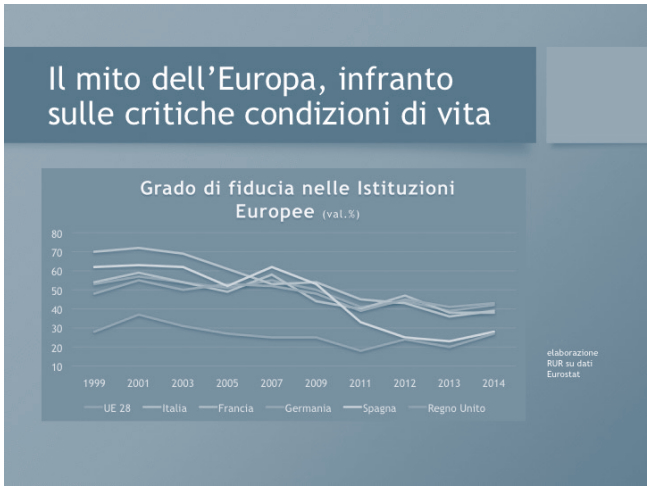
Se guardiamo poi all'impatto delle tecnologie della comunicazione vediamo che l'utilizzo che viene dagli europei più consigliato e comunque accettato dagli europei è quello che riguarda l'azione delle istituzioni per la sicurezza. Le tecnologie della comunicazione sulla sicurezza per oltre 60% degli europei sono strumenti che servono per l'azione delle forze di polizia, della magistratura eccetera, ma anche per garantire i diritti di libertà e la sicurezza dei cittadini. Gli italiani più o meno sono sulla stessa lunghezza d'onda.

La percezione in Italia della riduzione dei diritti di libertà è abbastanza in linea con l'Europa, però circa il 50% della popolazione che ritiene che, pur accettandola, ci sia una riduzione di diritti e delle libertà personali dovuta a questi interventi sulla sicurezza.

Per quanto riguarda la comunicazione, anche qui abbiamo un quadro non del tutto coerente, da una parte si dice - come risultato di un'indagine a livello globale - che ognuno deve potersi esprimere senza alcuna censura; in Europa questo vale per il 65% degli Stati Uniti per il 71%. D'altra parte però la maggior parte della popolazione, 59%, richiede che comunque le notizie sensibili vengano controllate, filtrate da parte del Governo e delle autorità quando sono notizie sensibili che inducono allarme sociale.

In pratica tutto il quadro che vi sto facendo viaggia a due velocità: da una parte si tende a ribadire i principi di coerenza con le proprie libertà personali e con la capacità di auto controllo, eccedendo nell'esposizione pubblica di se stesso, dall'altra resta una remora a rinunciare al proprio privato di fronte alla sicurezza come bene pubblico, irrinunciabile.

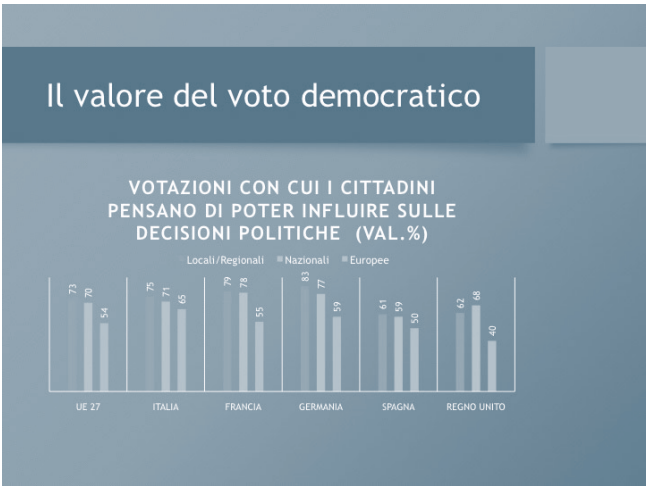
In conclusione, la democrazia vale proprio perché ha una flessibilità e può trovare un equilibrio fra quanto perdiamo in libertà e quanto guadagniamo in sicurezza. Certamente l'elemento cardine è la fiducia, ad esempio quando analizziamo la fiducia nei confronti delle istituzioni europee lo vediamo chiaramente declinare.



Le istituzioni europee in qualche modo sono la variante che ci ha tolto certezze: la sicurezza basata sugli Stati nazionali è una sicurezza molto più vicina al cittadino di quanto non sia una sicurezza ormai a più dimensioni, nazionali, locali, europee.

È chiaro che quando la fiducia nelle istituzioni europee, per esempio per gli italiani passa da circa il 70% dei primi anni 2000 al 54% del 2009 - cioè quando inizia la crisi - e poi al 39% del 2014, è evidente che si tratta di una discesa veramente preoccupante. Si può dire che gli italiani hanno paura della troika, e questo desta sfiducia, ma i dati sono simili in tutti i grandi paesi europei: noi siamo al 39% i francesi al 38%, i tedeschi al 43%, gli spagnoli al 28%, e gli inglesi sono sempre stati abbastanza scettici sull'Europa.

In questa dimensione complessiva, la democrazia come valore riconosciuto, la necessità della sicurezza come problema che va gestito nella molteplicità dei rischi, se si spostano i limiti e le possibilità di intervento a livello più ampio, cioè verso l'Europa e queste istituzioni ricevono scarsa fiducia da parte dei cittadini, si crea un pericoloso vuoto sociale. E bisogna ripartire dal valore da ridare alla rappresentanza e all'attenzione da riportare verso la costante partecipazione dei cittadini alla vita politica e istituzionale.



Concludo con una frase di Spinoza: "*Lo Stato democratico deve liberare dalla paura i suoi cittadini, però non può conseguire la sicurezza a scapito della libertà*". Credo che questo semplice pensiero è un principio che tutti noi possiamo condividere. La dimensione della democrazia come punto di riferimento della trasparenza, della responsabilità, della consapevolezza dell'informazione ai cittadini.

La democrazia come meccanismo che ci può garantire dagli eccessi di un controllo che non rispetta l'individuo. E' indispensabile combattere le insicurezze perché una società possa progredire, possa guardare al futuro con maggiore serenità. E alla fine, solo la pratica della democrazia ci aiuterà a uscire da questa dimensione di paura che sembra attanagliare la società europea.

Augusta Iannini

Grazie al professor Roma, perché attraverso i dati ha concretizzato una serie di elaborazioni anche filosofiche che erano state fatte nella prima parte della nostra mattinata. Quindi ci ha dato una risposta agli interrogativi che avevo posto prima. Sostanzialmente c'è una situazione di equilibrio, c'è consapevolezza della riduzione dei diritti, ma questa limitazione dei diritti viene

accettata dai cittadini in nome della sicurezza. Tuttavia, mi pare che il bilanciamento funziona se c'è fiducia nelle istituzioni e ciò significa anche la trasparenza delle modalità di gestione del potere.

Adesso passerei subito la parola al Procuratore della Repubblica di Torino, Armando Spataro. Non potrei sintetizzare il suo curriculum che è lunghissimo, quindi lo do per conosciuto. Si è occupato di tantissimi procedimenti di rilevante interesse, ma soprattutto dei processi per terrorismo, con interventi peculiari anche in tema di applicabilità del segreto di Stato.

Mi ha colpito che in numerose e recenti dichiarazioni abbia criticato l'ingorgo compulsivo di informazioni come inutile per le indagini, in particolare per le indagini sul terrorismo. Su questo punto penso che egli potrà darci delle indicazioni, anche con riferimento all'utilizzo di quei mezzi di indagine comunemente ritenuti particolarmente invasivi. Grazie.

Armando Spataro[1]

1) Premessa, brevi cenni al passato

Ringrazio il Presidente dell'Autorità Garante per la protezione dei dati personali per l'invito ad intervenire in questo qualificato consesso. Lo farò sulla base della mia esperienza di pubblico ministero, in particolare di quella maturata nel settore delle indagini sul terrorismo e di quelle, anche di diversa natura, che spesso si fondano su dati rilevanti che si possono acquisire attraverso la moderna tecnologia.

Naturalmente quella dei Pubblici Ministeri, quale io sono da quando sono entrato in magistratura, è un'ottica limitata, vista la finalizzazione del loro principale impegno (acquisire elementi di

(1) 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. Vi sono contenute citazioni, anche con aggiornamenti, da precedenti relazioni ed articoli.

prova circa le responsabilità di indagati e imputati per specifici reati), ma mi pare egualmente utile in questa sede - visto il tema in discussione - analizzare le modalità di lavoro e le potenzialità offerte dalle indagini fondate su raccolte ed analisi di dati personali, nonchè su intercettazioni telefoniche, ambientali e di comunicazioni telematiche.

Il tutto in un quadro più generale di corretta impostazione del contrasto al terrorismo internazionale.

Ritengo, però, di dover iniziare il mio intervento con 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 benchè 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 p.g. 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(2) e che consente di evitare sovrapposizioni di interventi forieri di equivoci ed errori.

(2) Il tema delle diverse competenze di P.G. e Servizi d'informazione verrà comunque trattato più avanti, anche con riferimento all'attualità.

2) 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 W.O.T. (*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(3). 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

(3) 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.

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 a loro carico.

In Francia esiste ancora la *"garde à vue"*, che consente alla polizia 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.

3) 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, tra cui il più importante è sicuramente il D. L. 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 c.p.), e prevedendo, sul versante procedurale, la competenza distrettuale per i reati con finalità di terrorismo, nonchè altre innovazioni atte a rinforzare le possibilità investigative(4).

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.

---

(4) 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):
  - 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.

• il D.L. 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 c.p.: tali condotte sono state tipizzate 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)(5).

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,

(5) 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 D.L.) 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 c.p. - e l'addestramento ad attività con finalità di terrorismo anche internazionale – ex art. 270 quinquies c.p. - 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).

sul presupposto di una delega politica, di richiedere di essere autorizzati dalle Procure Generali presso le Corti d'Appello allo svolgimento di intercettazioni preventive[6];

b) l'obbligo di identificazione degli acquirenti di schede elettroniche (S.I.M.) 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.

• il D.L. 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, nonchè dal CSM sin dal 2006. Sono stati dunque estesi al settore del terrorismo poteri e competenze del preesistente Procuratore Nazionale Antimafia[7].

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

(7) Non appare necessaria, in questa sede, l'illustrazione dettagliata del contenuto del D.L. 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, onvertito, 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.

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), di rimuoverli. Presso il ministero dell'Interno sarà tenuto un elenco aggiornato dei siti in questione[8];

b) con l'art. 7 del DL. n. 7/15, vengono previste *"Nuove norme*

(8) 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 e' aggiunto, infine, il seguente periodo: «La pena prevista dal presente comma nonchè dal primo e dal secondo comma è aumentata se il fatto è commesso attraverso strumenti informatici o telematici.»;

2) al quarto comma e' 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, nonche' delle attività di prevenzione e repressione delle attivita' 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

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:

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: «,nonchè al Comitato di analisi strategica antiterrorismo».

- 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'A.G. 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(9), che ha ferito

(9) 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 acquista 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.

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"*(10) 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(11). Francamente - e senza giri di parole - trovo queste posizioni inaccettabili.

Deve essere invece chiaro che la nostra democrazia non può tornare indietro di 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(12). Ma qui stiamo

(10) Corriere della Sera, 27 novembre 2015.

(11) Corriere della Sera, 4 dicembre 2015.

(12) 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.

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.

4) I dati personali, la loro diffusione e la loro raccolta a scopo investigativo

E' 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.

E' 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(13), *"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

(13) "Echelon e il controllo globale", Einaudi 2006.

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 predisposti da soggetti privati, dunque orientate da logiche meramente economiche ed aziendali: persino una direttiva sulla protezione cibernetica del gennaio 2013 dell'allora premier Monti(14), 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,

(14) DPCM 24 gennaio 2013 del Presidente del Consiglio pro tempore Monti: "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale".

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.

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.

5) **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.

5.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 riguarda 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"(15).

Con l'art. 3 c.1 del citato D.L. 18 ottobre 2001, n. 374, convertito nella Legge 15.12.2001 n. 438(16), 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

(15) Al riguardo, la disciplina originaria è contenuta nell'art. 13, D.L. 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.

(16) 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".

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.

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.

5.b) Intercettazioni a mezzo "virus"

E' 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. E' 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 d.d.l. di conversione del d.l. 7/2015, stralciato poi in Aula, con cui si intendeva modificare l'art. 266 bis del C.P.P.. 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.

5.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»[17]. 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 PG 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 D.L. 18 ottobre 2001, n. 374 approvato dopo l' "11 settembre" e convertito con Legge 15.12.2001 n. 438[18].

(17) 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.

(18) 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.

E' 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 costituzionale per i quali la legge stabilisce la pena della reclusione non inferiore nel minimo a cinque anni o nel massimo a dieci anni, nonché delitti di cui all'art. 270, terzo comma e 306, secondo comma, del Codice Penale"*)
- possono riguardare non solo le conversazioni-comunicazioni telefoniche, ma anche quelle cd. ambientali e quelle per via telematica (oltre che l'acquisizione dei tabulati telefonici e telematici).

Le intercettazioni preventive sono 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 G.I.P..

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 D.L. 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, c.p.p.) 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.

5.d) Le intercettazioni preventive dei Servizi di Informazione istituiti con Legge n. 801/1977 e riformati, quali Agenzie di Informazione, con L. 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 L. 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 D.L. 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 E.D.U. 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 Informazioni istituiti con Legge n. 801/1977, poi riformati con la L. 3.8.2007, n. 124 e quindi denominati Agenzie di informazione[19].

(19) 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 (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.

Naturalmente tocca all'A.G. 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".*

5.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 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 telefonia 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.

E' 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(20). 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 c.p.p. (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

(20) 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 C.P.P.) 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, purchè 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.

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 di attività investigative difensive o tramite istanza rivolta al PM(21), 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.

5.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,

(21) Ai sensi dell'art. 358 c.p.p., infatti, il PM è tenuto a svolgere accertamenti su fatti e circostanze a favore della persona sottoposta ad indagini.

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 - 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'AG) unitamente a quella di "intercettazione" dei contenuti effettivi della comunicazione; dati esterni e contenuti vengono poi trasmessi agli impianti installati nella procura 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 es., 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 "commerciali" (telefonate, sms, etc.) e per gli apparati mobili comprendono l'indicazione del ponte ripetitore agganciato al momento della chiamata.

Essi non comprendono pertanto i dati relativi alle celle ed ai ponti ripetitori agganciati dall'utenza mobile nel momento in cui questa, anche spostandosi, non effettua o riceve alcuna chiamata.

I telefoni cellulari quando sono accesi ed al loro interno è inserita una SIM card, anche se non effettuano chiamate, inviano periodicamente al ponte ripetitore più vicino dei segnali, che possono essere registrati solo se viene attivato un servizio di localizzazione.

Attualmente se tale servizio non è attivato non rimane alcuna traccia degli spostamenti effettuati dal telefono cellulare che non effettua o riceve chiamate.

5.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(22), 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 D.L. n. 374/2001, conv. nella

(22) 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. 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.

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 Gen. B. Mario Parente, espertissimo investigatore, già Comandante del ROS dei Carabinieri[23]:

"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

(23) 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).

risulta senza dubbio 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.

E' 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."

5.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[24] e, dall'altro, nel fatto che nel co. 2 si prevede l'estensione della originaria riserva di legge, fino a ricomprendervi regolamenti e decreti, quali atti che possano contenere indicazioni sui trattamenti di dati ai quali - purchè 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.

5.i) Giudizio di sintesi sul sistema italiano

La "rassegna" normativa che precede consente dunque di affermare che nel nostro sistema disponiamo di strumenti efficienti

(24) Art. 53-Ambito applicativo e titolari dei trattamenti
1. Agli effetti del presente codice si intendono effettuati per finalita' 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, nonche' di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati.

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 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, sta per essere varato 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 PM[25]. 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.

(25) Il provvedimento citato dal dr. Spataro è stato varato il 15 febbraio 2016.

6) 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 chiava 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 investigatori 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". E' 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, nonchè sulle estese acquisizioni di dati riguardanti cittadini italiani.

Molti autorevoli commentatori hanno già posto in evidenza la grave, estesa 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(26).

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

(26) 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'F.B.I. e la Apple, che ha rifiutato di "sbloccare" l'i-phone dell'autore della cd. strage di San Bernardino, coperto da un sistema di criptazione.

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*), Giovanni 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 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[27] 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?"*[28]

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* (c.d. 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*[29]*, sottolineando l'esigenza di*

(27) 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.

(28) 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".

(29) 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.

un'adeguata selezione del materiale investigativo, che non può certo fondarsi sulla pesca a strascico 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*(30)*"*, che non conosceva la *privacy*?

(30) 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).

E *"che cosa diventa la libertà di circolazione* - si domanda Stefano Rodotà[31]- *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?"*

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

(31) Stefano Rodotà : Dove finiscono i diritti in un paese di intercettati? (La Repubblica, 25.7.06).

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.

E' 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.

7) **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[32] 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

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

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 Stefano Rodotà(33), 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* (attualmente in discussione nel Parlamento americano), che estenderà ai cittadini europei - se approvata - alcune garanzie per i trattamenti dei loro dati da parte delle autorità statunitensi(34).

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.

8) Sentenze della Corte Europea dei Diritti dell'Uomo sulla illegittimità dei poteri attribuiti alle Agenzie di Informazione. Sentenze delle Corte Costituzionali tedescha 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

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

(34) La Judicial Redress è stata approvata definitivamente il 10 febbraio e promulgata dal Presidente Obama il 24 febbraio 2016.

utilizzo di "megadati". La Corte Europea dei Diritti dell'Uomo lo ha affermato in due recenti sentenze:

- la sentenza del 4 dicembre 2015 della Grand Chambre 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 anti-terrorismo 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 Corte 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 PM 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 su 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.

9) Le criticabili prospettive dell'Europa nel contrasto del terrorismo internazionale: si punta solo su megadati 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 Service 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"(35).

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'I.S. 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

(35) Così il Segretario Generale dell'Interpol, Ronald Noble, il 19.11.2005, in un meeting di studio tenutosi presso la N.Y. University.

poco recepita in Italia[36]), la Decisione Quadro del Consiglio 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[37]- 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

(36) 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 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.

(37) "Schedare i passeggeri è contro i Trattati UE. Il garante europeo boccia la stretta sui voli" (Repubblica, 10 dicembre 2015).

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 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.

E' 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![38]

Purtroppo, però, non è così che, nella realtà, funzionano le cose e potrei citare molti esempi, dalla scarsa e tardiva collaborazione

(38) 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.

di Belgio e Francia dopo la strage di Parigi del 7 gennaio 2015 nella sede del periodico "Charlie Hebdo", allorchè, 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(39).

10) 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(40), costituirebbe un grande passo avanti. Per di più, estendendo gradualmente le sue competenze fino ad occuparsi anche dei reati di terrorismo internazionale(41), 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,

(39) 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.

(40) 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)

(41) 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", versione online, del febbraio 2015.

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).

11) La risposta giudiziaria e 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 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.

E' 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. Proprio domani, il 19 gennaio, la Presidente Laura Boldrini presiederà 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.

Augusta Iannini

Un intervento appassionato quello del procuratore che provo a sintetizzare in due parole. L'equilibrio si realizza attraverso le corrette modalità di utilizzazione di tutti questi dati, sulle quali, nei sistemi democratici, deve vigilare la magistratura. Certamente la diversità degli ordinamenti giudiziari non facilita la cooperazione giudiziaria: questo è un problema che si trascina ormai da decenni.

Io credo che anche la Procura europea - la cui istituzione è auspicabile - risentirà moltissimo della differenza tra ordinamenti giudiziari e bisogna anche dire che il nostro, nel suo genere, è un unicum, ma non lo dico in senso critico.

Adesso passo la parola al Sottosegretario Minniti, che non ha bisogno di presentazioni. I suoi incarichi politici ne disegnano il

profilo di grande esperto in tema di sicurezza, però la sua laurea in filosofia e, mi dicono, il suo amore per le poesie di Catullo, lasciano ben sperare che darà un approccio anche umanistico al suo intervento.

Grazie.

Marco Minniti

Innanzitutto vi ringrazio per l'invito, dato che non è usuale che a una iniziativa organizzata dal Garante della privacy venga invitata l'Autorità delegata alla sicurezza del Paese, e cioè l'organo politico che si occupa dei servizi segreti. Sembrerebbe quasi una contraddizione in termini. So di dovermi muovere in una situazione che può apparire particolarmente complessa, come voi vedrete, invece, non mi sento assolutamente a disagio, né per il parterre della tavola rotonda, né per coloro che mi stanno ascoltando in questo momento.

Prima di entrare nel dettaglio di quello che penso rispetto a quanto detto dal professor Roma, dalla professoressa Iannini e dal dottor Spataro - che è un pezzo di storia della lotta al terrorismo in questo Paese -, consentitemi di fare una brevissima valutazione analitica sulle minacce che abbiamo di fronte. Conoscere le minacce con cui ci dobbiamo confrontare è fondamentale per capire come contrastarle.

È stato detto, ne ha parlato per ultimo il dottor Spataro, che il nostro Paese ha una storia di lotta contro il terrorismo. È una cosa molto importante, da rivendicare come uno straordinario patrimonio. Per due ragioni: primo, perché è un patrimonio di comportamento investigativo, di conoscenze che sarebbe sbagliato non tenere oggi nella giusta considerazione; in secondo luogo, perché quella lotta al terrorismo noi l'abbiamo vinta.

Siamo uno dei pochi Paesi al mondo ad aver svolto un'azione di contrasto molto forte alla sfida lanciata dal terrorismo interno alla

nostra democrazia, e quella sfida l'abbiamo vinta. Questo non vuol dire che ora non sussistano segmenti di piccolo terrorismo interno, ma non c'è più alcun dubbio che l'epicentro della minaccia alla vita democratica italiana negli anni '70 e '80 è stato radicalmente sradicato. Se fate mente locale e andate in giro per il mondo, comprenderete che non ci sono molti Paesi che hanno affrontato una tale sfida e l'hanno vinta.

È altrettanto giusto sottolineare che abbiamo vinto quella sfida senza derogare a princìpi fondamentali della nostra democrazia. Tuttavia oggi abbiamo di fronte una minaccia terroristica che è radicalmente diversa rispetto a quella vissuta in passato. Diversa non solo e non tanto perché quello di allora era un terrorismo interno, mentre questo è un terrorismo internazionale, ma perché anche dentro l'ambito del terrorismo internazionale affrontiamo una fattispecie che non ha mai avuto precedenti nella storia del pianeta.

Il Presidente Soro lo ha già accennato, abbiamo di fronte un'organizzazione terroristica (non a caso si chiama Islamic State), che è capace nel contempo di portare avanti la componente simmetrica (ovvero l'attività militare relativa alla conquista di territori e la gestione di territori e sovranità in Siria e in Iraq), e quella asimmetrica (cioè la capacità di muoversi oltre i confini medio orientali e che è quindi capace di colpire in Australia, in Europa, in Africa e in Asia).

E' una minaccia assolutamente inedita, e rispetto a questo dobbiamo commisurare il grado della risposta.

Uno degli elementi fondamentali dell'attività asimmetrica di Islamic State è rappresentato dalle azioni di coloro che si radicalizzano nell'Islam. A volte teniamo discussioni abbastanza aspre per quanto riguarda i luoghi di culto collettivi delle varie religioni, ma la verità che conosciamo è un'altra, e cioè che la stragrande maggioranza di coloro che si sono convertiti e poi radicalizzati, lo hanno fatto sul Web e non frequentando luoghi di culto collettivi. Questi, in quanto tali, sono luoghi socialmente controllati. Nel momento in cui molte di queste persone si

avvicinano ad una moschea, ad esempio, è del tutto evidente che il messaggio che viene trasferito in quei luoghi è conosciuto.

Comprendete tuttavia quanto sia drammatica la questione di una radicalizzazione, di una conversione, che avviene attraverso il rapporto tra l'uomo e uno schermo. Io sono cattolico, ognuno di noi ha il proprio credo e chi si converte o si avvicina ad una fede religiosa, lo fa in modo tradizionale: stabilisce cioè un rapporto con la religione attraverso la frequentazione dei luoghi di culto, come la chiesa, il seminario, i boyscout. È chiaro che, diversamente, non c'è nulla di più drammatico di una conversione e di una radicalizzazione che avvengono in maniera solipsistica: un soggetto che da solo guarda un video mediante un dispositivo elettronico. Tutto questo non può essere sottovalutato.

La seconda questione: abbiamo di fronte una minaccia che ha la capacità di muoversi sul terreno globale, dobbiamo pertanto necessariamente sviluppare delle forme di coordinamento. Il punto cruciale della sfida è capire quale obiettivo il terrorismo intende raggiungere.

Gli obiettivi della sfida di Islamic State sono numerosi. Uno di questi sta nella stessa parola Islamic State: quando Islamic State compare sullo scenario mondiale, si presenta con un acronimo più lungo, ISIS ovvero *"Stato Islamico dell'Iraq e del Levante"*. In buona sostanza, nella sua fase nascente - il professor Roma lo ha definito lo stato nascente del movimento - Islamic State stabilisce un collocamento territoriale, l'Iraq e il Levante, ovvero quei territori antichi della mezzaluna fertile che rappresentano la culla dell'umanità.

Progressivamente ISIS cambia nella forma, ma soprattutto nella sostanza, diventa quindi IS, o DAESH come lo chiamano in arabo. Non si tratta soltanto di esigenze di comunicazione, ma c'è un obiettivo specifico, un programma chiarissimo: lo Stato islamico da quel momento non ha più confini. L'obiettivo dello Stato islamico, infatti, è quello di andare ovunque. Oggi lo chiamano il *califfato mondiale*.

Dobbiamo quindi comprendere che in questa sfida una questione drammatica impatta non soltanto le democrazie europee ma anche le grandi democrazie del pianeta. A questa sfida straordinaria come risponde una democrazia? Snaturando se stessa? Perdendosi? Questo è il quesito cruciale. Se una democrazia risponde snaturando se stessa, ha già perso, è già finita ancora prima di cominciare.

E' evidente che questo è un tema da maneggiare con grande attenzione; allo stesso modo va trattato il tema della paura. Stiamo parlando di un altro aspetto della sfida che viene lanciata da IS alle grandi democrazie. Bisogna chiedersi per quale ragione Islamic State commette quelle esecuzioni così drammaticamente violente.

Io, però, vorrei comprendere per quale ragione la violenza viene così esaltata e soprattutto vorrei capire per quale motivo l'informazione dà tanto spazio a questo modo di comunicare. Ho saputo, con grande piacere, che molti giornalisti hanno detto: "fermiamoci un attimo, quelle immagini non le passiamo più".

A tale proposito vorrei trasmettervi un altro messaggio, quando si usa la violenza in maniera così icastica, è perché si vuole insinuare un messaggio specifico, quello della paura.

Non si tratta di polemica politica (chi conosce il mio ruolo sa che io partecipo pochissimo alla polemica politica, anzi quasi mai, perché ritengo che per il mio ruolo non debba farlo) ma della necessità di comprendere fino in fondo che se in una democrazia vince la sindrome della paura, la stessa democrazia risulta più fragile e più debole. La sindrome della paura è uno degli obiettivi delle organizzazioni terroristiche. Se è così, è chiaro ed evidente che una grande democrazia risponde alla sfida del terrorismo con la fermezza necessaria.

Poi c'è una sfida che riguarda la sovranità, che riguarda il nostro stare insieme come comunità. So bene quanto sia facile rispondere sulla base dell'emotività, ma una grande democrazia non risponde sulla base dell'emotività.

Tengo molto conto delle analisi che ha fatto il professor Roma, per me sono molto importanti, però vorrei dirvi una cosa:

una grande democrazia non risponde utilizzando i sondaggi. Non c'è un problema di sondaggi di opinione sulle grandi questioni. Poi a me serve quello che ha fatto il professor Roma, perché mi dà un quadro della sensibilità del Paese, ma guai se il decisore politico dovesse prendere decisioni sulla base dei sondaggi nella lotta al terrorismo.

Il decisore politico deve essere pronto ad assumersi tutte le responsabilità e adottare le misure più efficaci, non quelle che sono "sulla cresta dell'onda", perché noi sappiamo che l'onda è una cosa che va via molto velocemente e stare sulla cresta dell'onda non è sempre semplicissimo. Sono molto convinto di ciò.

Dopo Charlie Hebdo il Governo ha emanato un decreto sulle misure più efficaci di lotta contro il terrorismo e non c'è dubbio che questo decreto abbia prodotto dei risultati: il nostro è un Paese che oggi ha una Procura nazionale antiterrorismo (Dio sa per quanto tempo l'abbiamo voluta e poi finalmente l'abbiamo realizzata), abbiamo alcuni strumenti che ci consentono insieme di prevenire e di reprimere, come, ad esempio, contro l'auto-addestramento (nei giorni scorsi sono stati fatti alcuni arresti proprio sulla base del fatto che in Italia è proibito l'auto-addestramento). Tuttavia penso che accanto al merito sia stato più importante il metodo con il quale si è giunti a quella determinazione. Penso di non fare nessuna rivelazione di segreto d'ufficio nel dire che mentre si discuteva del decreto antiterrorismo il Consiglio superiore della Magistratura ha convocato una riunione in cui c'erano i magistrati, il Garante della privacy, il dottor Spataro, indegnamente c'ero pure io a rappresentare il Governo.

C'è stata una discussione approfondita e l'obiettivo non era quello di vedere come stare sulla *cresta dell'onda*, ma creare delle misure efficaci che consentissero una coesione del Paese, che non apparissero come un elemento di competizione e di tensione dentro le Istituzioni fondamentali della democrazia italiana. Si è proceduto in questo modo e così, a mio avviso, bisognerà procedere progressivamente. Ovvero, di fronte alla sfida contro la democrazia,

una democrazia reagisce utilizzando al massimo gli strumenti di coesione.

Non vorrei portare nocumento all'Istituzione del Garante della privacy perché sono molto attento, essendo tra l'altro un ospite, a non voler nuocere al padrone di casa, ma la notizia è pubblica e quindi la posso riferire: l'intelligence italiana, qualche anno fa, ha stipulato un protocollo d'intesa, che finora è stato rispettato e continuerà a esserlo, con il Garante della privacy. Non era una scelta soltanto di merito, ma anche di metodo. Posso dirvi che non ci sono paragoni al mondo.

Penso anche che quanto detto dal Presidente Soro e dalla dottoressa Iannini ci dice con grande chiarezza che non abbiamo un Garante della privacy "abbastanza permissivo". Voglio dire che non è un garante della privacy che fa finta di non vedere, com'è giusto che accada in una democrazia, perché la democrazia è fatta di controlli, di pesi e di contrappesi, di gente che fa e di gente che controlla quelli che fanno. Questa è la democrazia. Questa è la differenza che c'è fra la democrazia e i poteri assoluti, perché - vorrei ricordare, come ha detto la dottoressa Iannini - che io, che nella mia precedente vita mi occupavo di filologia classica, so cosa vuol dire essere "sciolto". Vuol dire che non risponde a nessuno. La democrazia vincola e stabilisce che un soggetto debba reciprocamente misurarsi con l'altro.

Su questo vorrei fare due osservazioni di merito, la prima è questa: la dottoressa cita un uso massiccio e massivo dei dati. Su questo tema è ritornato anche il dottor Spataro. Io esprimo con chiarezza la mia opinione: innanzitutto, come voi sapete, in Italia non c'è raccolta massiva di dati. È proibita dalla legge. Posso anche aggiungere una cosa più sul merito. La mia idea è questa: Charlie Hebdo e poi il 13 novembre, ma tutte le altre vicende ci pongono una questione gigantesca cioè la fragilità dell'idea che il contrasto a organizzazioni così complesse come quelle terroristiche possa avvenire soltanto attraverso l'uso della tecnologia. Se ci pensate bene, questo è il cuore della questione. Se voi guardate le immagini del

post Charlie Hebdo e del post 13 novembre vedrete che non è un problema di raccolta dati, ma di quello che tecnicamente si chiama Humint, la conoscenza diretta ovvero stare dentro, conoscere da dentro.

Guardate, non è così semplice capire quello che succede pensando di controllare i dati. Quando in realtà si ha a che fare con il fattore umano, (humint appunto), è particolarmente complicato da gestire, e non può essere fatto soltanto attraverso un incrocio dei dati, ma attraverso l'incrocio di conoscenze. Bisogna, cioè, fare indagini.

Noi abbiamo un punto di forza che ci deriva dalla storia dell'Italia, (e mi auguro che venga veramente fatto in Europa), un centro unico, si chiama CASA. L'acronimo sta per *Comitato Analisi Strategica Antiterrorismo*. È un unico centro in cui attorno allo stesso tavolo sono seduti i rappresentanti delle forze di polizia e i rappresentanti dell'intelligence. Peraltro oggi abbiamo un altro interlocutore, ovvero la Procura nazionale antiterrorismo.

Qual è il punto di forza del CASA? Intorno a quel tavolo che si riunisce settimanalmente - e in casi di emergenza ogni giorno - si scambiano immediatamente e in tempo reale tutte le informazioni. In tempo reale, sapete che cosa significa questo? Vuol dire sviluppare una straordinaria capacità di produzione.

Tuttavia risulta con evidenza che lo scambio di informazioni rappresenta il punto cruciale che a volte mostra la fragilità in termini di capacità della risposta. Dopo l'11 settembre gli Stati Uniti hanno creato una commissione d'inchiesta dalla quale è uscito fuori che ciò che è mancato non erano tanto i sensori, quanto lo scambio reciproco di informazioni. In quel caso la sfida, che in qualche modo era stata percepita, era stata considerata troppo radicalmente forte da poter essere considerata credibile. Se qualcuno avesse detto prima dell'11 settembre che sarebbero stati dirottati quattro aerei e mandati contro le Twin Towers, il Pentagono e la Casa Bianca, sarebbe apparsa un'operazione altamente improbabile. Il problema è che al-Qaeda allora fece proprio lo slogan del maggio francese: *"siate*

realisti, pensate l'impossibile". Il massimo del realismo era pensare l'impossibile, la tragedia è che loro non solo l'hanno pensato, ma l'hanno realizzato.

Infine un'ultimissima considerazione, anche questa sul merito: in Italia esiste un sistema di bilanciamento. Sono d'accordo con quanto detto dal dottor Spataro sul know-how straordinario delle forze di polizia italiane, l'intelligence è un'altra cosa. Deve sviluppare di più la capacità produttiva, ma naturalmente collabora con le forze di polizia. In Italia l'intelligence ha poteri straordinari, com'è giusto che sia, in base a una legge approvata dal Parlamento, ma questi poteri sono regolati da procedure.

In democrazia le procedure e le formalità sono elementi fondamentali, la democrazia è procedura e formalità. I poteri straordinari in Italia sono regolati da una doppia chiave: l'intelligence può fare alcune cose se il Governo se ne assume la responsabilità e se sono autorizzate dalla magistratura. Poi c'è il Parlamento che controlla quello che si fa, in un bilanciamento preciso. C'è bisogno di snaturare tutto ciò? Assolutamente no. Io penso che questo sia un modello che ha funzionato e quindi non c'è bisogno di "andare oltre".

Concludo dicendo che tutto questo comporta la gestione attenta dei poteri. Io penso che il PNR, *passenger name record*, così come sta per essere varato dall'Unione Europea e dal Parlamento europeo, tenga in equilibrio le esigenze di custodire un patrimonio di carattere investigativo e quelle della privacy.

Il Parlamento europeo ha all'attenzione questo tema da oltre due anni, quindi non stiamo parlando di scelte affrettate. Voi comprendete perfettamente che nel momento in cui c'è il tema dei *foreign fighters*, avere una banca dati per sapere chi viaggia e chi non viaggia dalla Siria verso l'Europa e dall'Europa verso la Siria, non è una cosa sconvolgente. A volte succede che qualcuno decida di incontrarsi per ragioni di riservatezza per esempio stando seduti l'uno accanto all'altro in aereo. Chiedere chi sta seduto accanto all'altro può essere un elemento che permette di comprendere ciò

che è avvenuto, a me non pare che sia un punto sul quale dobbiamo sconvolgere il ragionamento che ho fatto fino a qualche secondo fa.

Se qualcuno mi chiede: ma tu, come persona, non soltanto come rappresentante del Governo, come pensi possa essere affrontato il tema sicurezza e libertà? Io rispondo con una nettezza che vorrei fosse inequivoca: dobbiamo guardarci, in democrazia, da coloro che pongono il tema di uno scambio radicale tra sicurezza e libertà; non c'è la possibilità, in democrazia, di scambiare alcunché su questo terreno.

Posso dirvi una cosa, la mia opinione è molto radicale. Per me tra sicurezza e libertà non solo c'è una connessione, ma quella *"e"* che congiunge sicurezza e libertà è una *"e"* con l'accento, proprio perché sono due facce che stanno strettamente insieme. Per essere più chiari la dico così: è evidente che non ci può essere alcuna libertà se non c'è una sicurezza. E' chiaro che se vengo minacciato nella mia vita quotidiana, perdo un pezzo della mia libertà, ma voi comprenderete anche a che mi serve la sicurezza se poi io vengo ridotto come individuo sociale? La democrazia è fatta di individui sociali, se ci pensate bene la sfida del terrorismo è quella di rompere quei vincoli sociali; è quella di rompere quel riconoscimento reciproco tra individui che è il fondamento delle ragioni di una democrazia.

Per questo vorrei concludere soffermandomi su un punto cruciale, quello della sfida vera che abbiamo di fronte: i terroristi del radicalismo islamico pensano che l'opinione pubblica sia un punto di fragilità della nostra democrazia. L'idea dell'incalzare con l'attività terroristica e con un gesto simbolico fortissimo ha questo obiettivo.

I terroristi pensano che una classe dirigente della democrazia deve rispondere alla propria opinione pubblica e quindi se l'opinione pubblica si sente direttamente minacciata o addirittura impaurita, è chiaro che quella classe dirigente perde forza.

Io la penso in maniera esattamente speculare rispetto alla visione dei terroristi. Per me l'opinione pubblica è un punto di forza

di una democrazia ed è per questo che la sfida contro il terrorismo noi la vinceremo soltanto con il consenso, con il protagonismo, con la capacità di far sentire ogni individuo sociale protagonista.

Se facciamo così noi la partita la vinciamo, se facciamo in un altro modo, guardate, noi abbiamo già "rinsecchito" noi stessi e quindi combattiamo con le mani dietro la schiena.

Di fronte ad una discussione che si è aperta, cito uno dei più grandi, uno di quelli che ha fatto fare il salto più grande all'intelligenza artificiale, Alan Turing (lo ricordo sempre perché è morto in una maniera drammatica), che era convinto che l'intelligenza artificiale ad un certo punto potesse sostituirsi a quella umana. Io, che lo ammiro tantissimo, su questo so perfettamente che sbagliava: non c'è nessuna intelligenza artificiale che può sostituire l'intelligenza umana.

Augusta Iannini

Grazie, a questo punto passo rapidamente alla seconda tavola rotonda, coordinata dalla dottoressa Bianchi Clerici.

Condivisione, profilazione, Big Data

Sessione II

Guido Scorza
Avvocato

Fabio Chiusi
Giornalista

Maurizio Ferraris
Filosofo

Moderatore **Giovanna Bianchi Clerici**
Componente del Garante
per la protezione dei dati personali

Sessione II

Condivisione, profilazione, Big Data

Giovanna Bianchi Clerici

Signori, vi pregherei cortesemente di accomodarvi perché siamo in leggero ritardo sui nostri tempi e quindi avremmo bisogno di cominciare. Il tema della sessione è: *"Condivisione, profilazione, Big Data"*.

Ho pensato, per introdurre il tema e gli interventi dei nostri ospiti, di mostrarvi sei o sette slide che servono semplicemente a definire un po' i contorni del tema di cui ci occupiamo oggi. Slide che abbiamo realizzato in maniera assolutamente artigianale con la preziosa collaborazione dei ragazzi che lavorano nel mio ufficio e che si sono improvvisati grafici, per cui magari non saranno impeccabili dal punto di vista tecnico, ma credo siano utili a definire un po' il problema.

"*Condivisione, profilazione e Big Data*". Per inquadrare questo tema siamo ricorsi ad una formula piuttosto nota che è quella delle tre V: Volume, cioè grandi quantità di dati; Varietà, quindi tipi diversi prodotti da numerose fonti, a grande Velocità.

Sostanzialmente stiamo parlando di quelle tracce digitali che noi tutti lasciamo in maniera anche inconsapevole, quali le foto, i commenti, i video, le mail e le ricerche che facciamo sui siti.

In realtà siamo in presenza di quello che è stato definito da Bauman *"uno tsunami di dati"*.

Quanti dati vengono prodotti oggi?

La stima più approssimativa, più corretta probabilmente più vicina a quella reale, è di 2,5 miliardi di miliardi di bytes.

Che cosa ci riserva il futuro?

Viene stimato che entro il 2020 arriveremo a 40.000 miliardi di miliardi di bytes.

Questa immagine, che rappresenta l'onda cartacea per eccellenza, ci è piaciuta per descrivere questo tsunami che invece è digitale.

I dati che vengono conservati oggi in formato digitale, rappresentano il 99,5% dei dati prodotti dall'uomo, pensate che solo il restante 0,5% ricomprende i dati analogici a cui eravamo tutti abituati, dunque libri, registri cartacei eccetera.

La Velocità: i dati on-line possono essere raccolti e registrati come sappiamo tutti a milioni di risultati per secondo; algoritmi sempre più sofisticati sono in grado di predire il comportamento degli utenti in microsecondi.

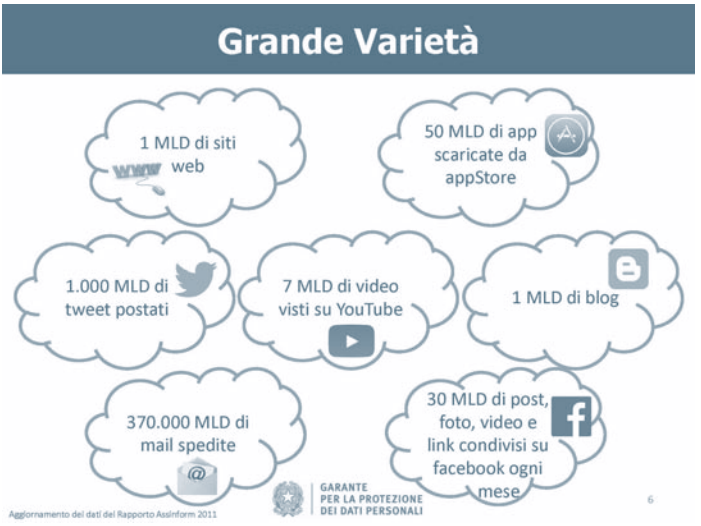
Questa è l'immagine di che cosa accade, questo grafico che ci dice cosa accade on-line in 60 secondi, credo sia assolutamente in grado di farci comprendere bene il fenomeno.

Guardate per esempio Google: siamo passati da poco meno di 700.000 ricerche al minuto che venivano fatte nel 2012, ai 4 milioni del 2014, e ciò perché il dato più recente che abbiamo avuto è questo.

Possiamo parlare decisamente di un balzo incredibile.

La stessa cosa per Facebook: da poco meno di 80.000 nel 2012 (sempre al minuto), siamo a 3,3 milioni ogni 60 secondi.

La Varietà è ovvia, viene dai siti, dai *tweet* postati, dai video di Youtube, dalle mail spedite, dai blog e non dimentichiamo quel segmento sempre più importante del cosiddetto *"Internet delle cose"*, ossia tutti i dati di tipo ambientale che arriveranno sempre più massicciamente dagli elettrodomestici, dalle automobili, dall'illuminazione pubblica, da tutti questi dispositivi intelligenti che sono connessi e saranno sempre più un'estensione di noi stessi, (es. il fenomeno di quella realtà aumentata che è sempre più una realtà).



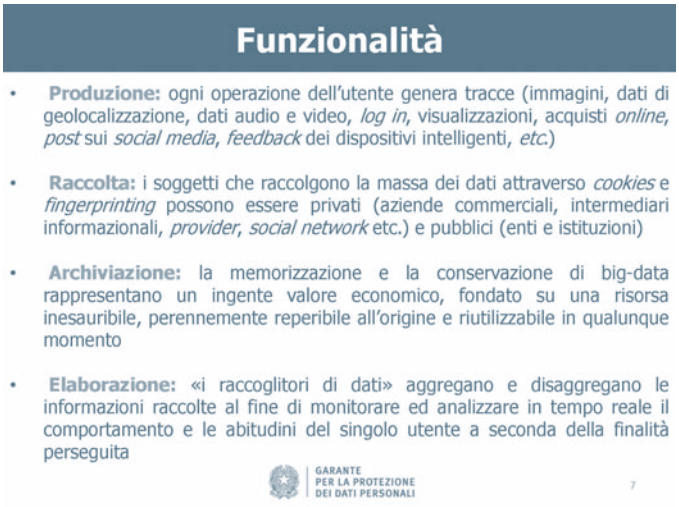
Come opera?

Lo ricordiamo che è semplicemente, una produzione: ogni operazione dell'utente genera delle tracce, immagini, dati di geolocalizzazione, dati audio e video, *log in*, visualizzazione, *feedback* dei dispositivi intelligenti.

La raccolta: i soggetti, che raccolgono la massa di dati attraverso i *cookies* e attraverso i *fingerprinting* introdotti nei nostri terminali dai sistemi, quindi non maneggiabili da tutti noi, dall'utente stesso.

I soggetti sono sia privati, (le aziende di intermediari informazionali, *social network* eccetera) e sia pubblici (istituzioni e agenzie governative).

La memorizzazione e la conservazione di tutta questa mole enorme di dati rappresenta un ingente valore economico, fondato su una risorsa inesauribile, perennemente reperibile all'origine e riutilizzabile in qualunque momento.



I raccoglitori di dati, aggregano e disaggregano le informazioni raccolte al fine di monitorare e realizzare in tempo reale il comportamento e le abitudini del singolo utente, a seconda della finalità che viene perseguita. La profilazione, il risultato dell'elaborazione di questa enorme mole di dati è "un'identità digitale" corredata di tutte le caratteristiche uniche che individuano un utente fra miliardi. L'attività di profilazione si basa su infinite combinazioni di dati, talmente accurate da generare per un singolo utente addirittura due identità che lo rappresentano negli aspetti della sua vita quotidiana: il profilo professionale e quello personale.

I pro: sono già state in parte citate le opportunità economiche ed occupazionali, tra le quali: semplificazione della vita, previsioni più accurate in politica, nel mercato, nella salute, nel traffico e, non ultimo, una potenziale riduzione dello spam.

Di contro: un uso improprio dei dati, un eccessivo controllo della vita privata, un'estrema settorialità e limitazione delle scelte, un'autoreferenzialità che diventa veramente eccessiva talvolta, una passività dell'utente e una potenziale discriminazione.

Bene, è di questi temi che vogliamo parlare con gli ospiti, a cominciare con dall'avvocato Guido Scorza, che si occupa prevalentemente di diritto dell'informatica e proprietà intellettuale, materie che insegna all'università di Bologna e alla Lateranense. È titolare dello studio legale E-lex ed è anche Presidente dell'Istituto per le politiche dell'innovazione. Scrive per alcuni quotidiani e periodici, ha un blog su alcuni giornali, tra cui Il Fatto quotidiano, Il Sole 24 Ore e l'Espresso. Collabora inoltre con la Presidenza del Consiglio per l'attuazione delle politiche di innovazione.

Avvocato, io Le sottoporrei una domanda: l'avvento dei Big Data, con tutti questi cambiamenti che comporta e con i rapporti asimmetrici di forza tra chi produce il dato e i soggetti che invece lo elaborano e lo analizzano, rischia di rendere forse superato il tradizionale

principio cardine su cui è stata impostata, in ambito giuridico, la protezione dei dati personali, ovverosia il paradigma informativa-consenso. Questo è un tema che, come Lei può comprendere, è molto interessante per noi, per cui Le suggerirei anche questo spunto, se è possibile.

Grazie.

Guido Scorza

Grazie all'Autorità garante per l'invito, è un'occasione di confronto straordinaria.

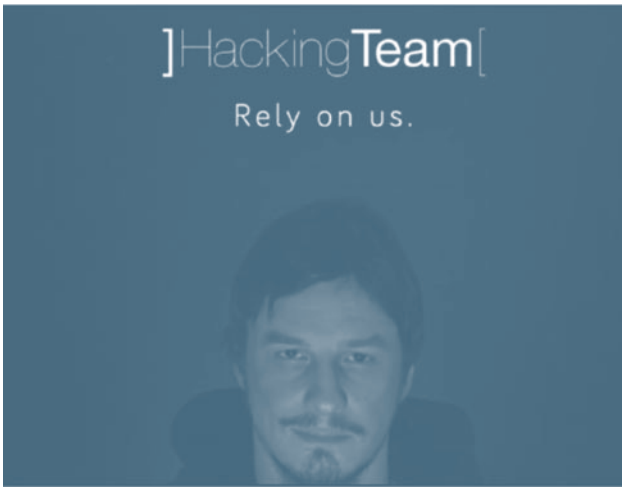
Io parto da lontano, naturalmente con l'ambizione di arrivare in fretta a vicino. Per quanti si occupano di privacy, la storia della privacy inizia lì: "Il più povero degli uomini può, nella sua casetta, lanciare una sfida opponendosi a tutte le forze della Corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il Re d'Inghilterra non può entrare. Tutte le sue forze non osano attraversare la soglia della casetta in rovina". Era il 1766, era Lord Chatham davanti al Parlamento inglese.

Noi oggi siamo qui esattamente duecentocinquant'anni dopo e io credo che qualsiasi riflessione sulla tutela dei dati personali debba iniziare dall'analisi di come il diritto sui propri dati viene percepito.

Permettetemi di rompere l'istituzionalità con una vignetta satirica che talvolta – racconta più di tante parole: "Lo scandalo della NSA", il personaggio della vignetta dice "Ascoltiamo tutto, questa è la costituzione degli Stati Uniti d'America, non l'avevo mai letta".

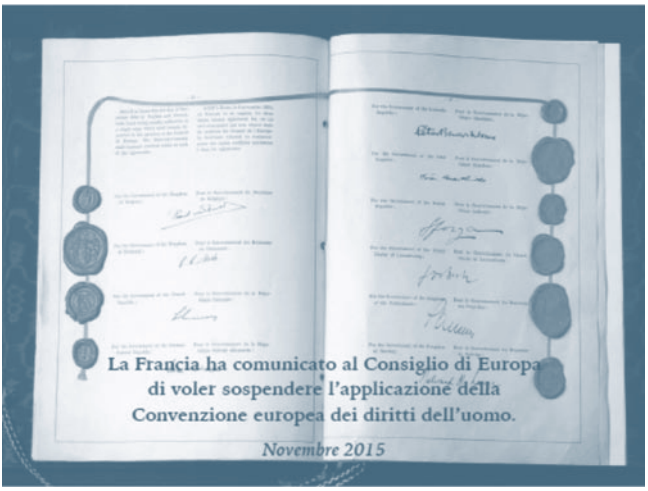
Sbaglieremmo però, a puntare l'indice dall'altra parte dell'oceano, quasi a dire che c'è uno scontro tra culture: Europa contro Stati Uniti. Francamente di questo scontro, ammesso che sia mai esistito, oggi si fa davvero fatica a rintracciare il patrimonio genetico.

La vicenda dell'Hacking Team: questo è uno *screenshot* di uno spot di quella società di cui tutti abbiamo sentito parlare, tutta privata, che vendeva prodotti e, ciò che è peggio, a quanto pare servizi, a soggetti governativi e non governativi. Un ricercatore e attivista californiano due anni prima che lo scandalo deflagrasse qui da noi era salito sul palco di un TED negli Stati Uniti e aveva detto: "Trovo strano che Hacking Team - e non solo Hacking Team, anche la Gama tedesca - se ne vadano in giro per il mondo a fare pubblicità e a finanziare coffee break di agenzie di intelligence per vendere i loro prodotti".



Racconto questa vicenda non per analisi giuridica ma per guardare, viceversa, al percepito. È scorsa via con poche eccezioni sui giornali e nei media e secondo me l'opinione pubblica italiana più di tanto non si è scandalizzata di qualcosa che pure è accaduto dentro casa. L'abbiamo già sentito ripetere in apertura di questa nostra chiacchierata oggi, più volte: ha fatto poca notizia persino la Francia che, a ridosso di fatti certamente scioccanti come gli attentati di Parigi, scrive una lettera e dice: "Per me la Convenzione

internazionale sui diritti dell'uomo, per rispondere in maniera efficace al terrorismo, è troppo stretta: scelgo di uscire".



Per la prima volta nella storia, cinque relatori speciali delle Nazioni Unite nei giorni scorsi hanno preso carta e penna e scritto al governo di Parigi dicendo "Siamo preoccupati". Uno dei cinque relatori è il nuovo relatore speciale delle Nazioni Unite per la promozione e tutela della privacy, il professor Cannataci, che in particolare punta l'indice esattamente sulle cose delle quali abbiamo sentito parlare sin qui, cioè su un eccesso nella sorveglianza di massa, sulla famosa "scatola nera" che in una legislazione emotiva e di emergenza ha trovato posto nell'ordinamento francese.

Di Safe Harbor, se vogliamo parlare di valore dei dati, di Big Data, di profilazione, dobbiamo farci carico di discutere. Non c'è più niente, oggi, nel mercato dei dati personali che sia nazionale.

Tutti i mercati - e ancora di più quelli dell'immateriale - sono globali e naturalmente se non c'è scambio non c'è mercato. Eppure l'unica riflessione che io lascio, in questa maratona di parole, a proposito del Safe Harbor, è una: la mia perplessità è in quell'*hashtag*, nella fragilità. Abbiamo visto andare in frantumi perché un ragazzino ha portato puntato l'indice contro una decisione della Commissione europea un sistema che ha garantito per quindici anni, tra le perplessità di tanti, per non dire di tutti, non solo lo scambio di dati – e quindi il mercato – ma anche la privacy e i diritti fondamentali di centinaia di milioni di cittadini.

Oggi che si discute tanto del Safe Harbor 2.0, del nuovo Safe Harbor, devo dire che sono fortissimamente perplesso rispetto all'idea che un accordo di questo tipo possa davvero governare, anche se scritto meglio, anche se riscritto, lo scambio dei dati personali dei quali oggi discutiamo.

Anche di PNR abbiamo già sentito parlare, quindi di questa vicenda io prendo soltanto, ancora una volta, la reazione degli italiani e la prendo perché è sintomatica del valore che attribuiamo ai nostri dati personali, del significato che diamo

alla privacy, probabilmente in termini non statistici ma, in ogni caso, di percepito. Secondo me questo è un fattore, almeno culturalmente, molto importante.

A ridosso della decisione della Commissione del Parlamento europeo di aderire alla proposta dell'Unione europea, ho scritto, come penso abbiano fatto in tanti, un articolo nel quale dicevo che probabilmente stiamo davvero eccedendo in sorveglianza, raccogliendo dati che forse le agenzie di intelligence non riusciranno mai nemmeno a processare.

Queste sono alcune delle reazioni degli utenti a quell'articolo: "Dov'è il problema?, "Che m'importa se sanno dove vado, cosa mangio, cosa compro, se serve per la sicurezza di tutti va benissimo", "Telecamere in ogni angolo", "Non riesco proprio a capire come ci si possa sentire così profondamente violati nel mettere a disposizione delle forze dell'ordine alcuni dati ai fini della propria sicurezza, quando ogni giorno la gente si mette a sbandierare sui social media ogni più insignificante dettaglio della propria vita. Questa mi sembra solo ipocrisia"; poi il ritornello più ricorrente, "Male non fare, paura non avere", come a dire che se non ho niente da nascondere la privacy non è un mio problema.

Questo è il percepito degli italiani ed è un percepito che era stato anticipato - così passiamo dal pubblico al privato e ci avviciniamo anche al tema che mi è stato proposto – da mister Zuckerberg, mister Facebook: "Ormai gli utenti condividono senza problemi le informazioni personali on-line.

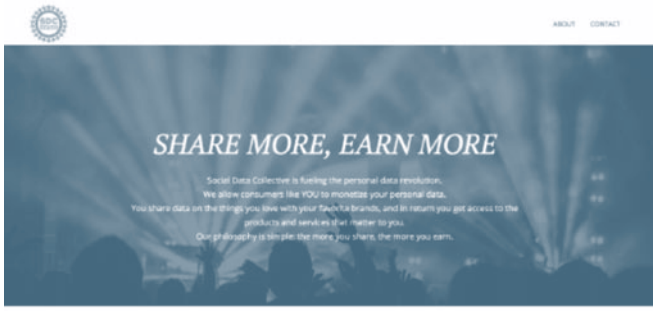
Le norme sociali cambiano nel tempo: è così anche per la privacy. Quando ho iniziato a pensare a Facebook, nella mia cameretta di Harvard, in tanti si chiedevano perché mai dovrei mettere informazioni on-line".

Poi è successo quello che tutti quanti sappiamo, abbiamo iniziato a condividere e qui è assolutamente inutile puntare l'indice verso chi tratta quei dati commercialmente.

È ovvio che il problema è un minuto prima ed è un problema di natura culturale, che viene dal basso e non dalle corporation. Chissà quanti di voi, soprattutto quanti si occupano più da vicino del problema delle basi di dati e del loro commercio, ha visto transitare sul suo pc una mail come questa: un'offerta tutto sommato scomposta, sia in termini commerciali che grammaticali, di acquisto o di vendita di base dati più o meno profilate, che sa più di mercato nero che non di mercato strutturato.

È fuori di dubbio, penso, che stiamo assistendo ad una vera e propria svalutazione della nozione di privacy, con la quale in qualche modo dobbiamo fare i conti, se vogliamo occuparci di regolamentazione e governo del problema. La privacy, per i più, sembra veramente diventata la moneta con la quale compriamo l'accesso a servizi di ogni tipo. Tutto sommato la sensazione è che troviamo persino equo il prezzo che paghiamo per usare i servizi, se paghiamo in dati personali.

C'è questa start-up americana, che non è né l'unica né particolarmente originale, che da poco ha avviato la sua presenza sui grandi shop di e-commerce che dice "share more, earn more": cioè l'idea sostanzialmente è "condividi i tuoi dati e io in cambio ti do dei buoni da spendere nei prodotti e nei servizi che più ti piacciono".



Una ricerca di mercato che hanno fatto prima di entrare sul mercato racconta che il 38% dei giovani tra i 18 e i 34 anni negli Stati Uniti scambierebbe volentieri il proprio consenso al trattamento per finalità commerciali alla privacy per un abbonamento settimanale alla metro. Questo dice molto della percezione della privacy tra i più giovani.

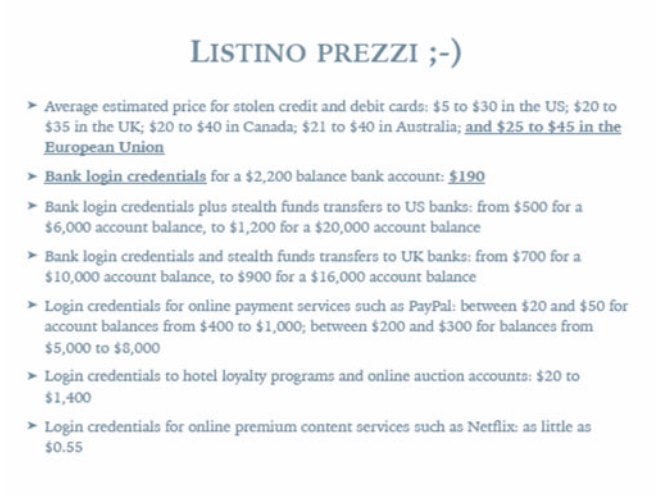
DATI PERSONALE, MERCE DI SCAMBIO

- The Social Data Collective surveyed people age 18 to 34 in the New York metropolitan area and discovered that *38 percent would exchange their personal data for a weekly subway pass*.

- A similar study from PriceWaterHouseCoopers determined that *63 percent of consumers age 18 to 59 would be interested in discounted movie tickets and 60 percent would accept a coupon for free food or beverages at a movie theater*.

Parliamo di dati personali e parliamo ormai essenzialmente di una merce qualsiasi, con questo dobbiamo fare i conti. Devo dire che ho fatto io stesso, in preparazione di questo nostro incontro, un test su un servizio messo a disposizione nel 2013 dal Financial Times. Ci sono rimasto molto male perché il servizio consente di misurare quanto valgono i tuoi dati personali, ti dice che la media è di un dollaro, sul mercato, mentre io ho raggiunto 0,2371 e la mia autostima è calata sotto i minimi storici: valgo meno della media del mercato e i miei dati valgono meno di un dollaro.

Non vi tedio sul mercato nero, il mercato parallelo dei dati personali, lo conoscete perfettamente. Anche lì in realtà il valore del dato personale, tradotto in numeri, in dollari, dà una percezione dalla quale non possiamo davvero sottrarci.



Qui discutiamo di quello che è nato come diritto fondamentale e che oggi è diventato uno dei tanti diritti di proprietà, assolutamente disponibili, disponibilissimi. Siamo soltanto all'inizio. Probabilmente molti di voi hanno già avuto modo di leggere lo studio dell'Organizzazione per la cooperazione e lo sviluppo pubblicato lo scorso anno, nel quale si parla della *"data-driven innovation"*, la *datafication* dell'economia.

Il costo di raccolta, *storage* e trattamento dei dati personali diminuisce sempre più e il valore di quei dati aumenta sempre più, il che significa che sotto il profilo economico è un processo assolutamente irreversibile.

Noi dobbiamo governare quello che è, allo stesso tempo, un terreno di diritti fondamentali e un mercato globale di enorme valore economico.

Lo stesso studio valuta, nel 2015, in 17 miliardi di dollari il mercato globale dei Big Data: è qualcosa con cui dobbiamo fare i conti.

IL COSTO DELLA RACCOLTA, DELLO STORAGE E DEL TRATTAMENTO DEI DATI DIMINUISCE CONTINUAMENTE

The datafication of economy and society

Mi avvio verso le riflessioni finali, ritenendo davvero che quella che abbiamo davanti – e che hanno in prima persona sul tavolo le *authority*, i governi, i parlamenti – è una partita straordinariamente difficile, perché è già difficile difendere un diritto fondamentale nel momento in cui i titolari hanno una percezione chiara del valore di quel diritto, quando i titolari di quel diritto non hanno quella percezione, quando, per di più, cultura e mercato ci convincono che non si tratta di un diritto fondamentale ma che si tratta, invece, di una merce di scambio, di mercato, devo dire che ho tutta la stima del mondo in questa Autorità e in quelle che in giro per l'Europa fanno lo stesso lavoro, però trovo davvero che la sfida che avete sul tavolo e noi, come comunità, con voi, sia difficile.

La tutela della privacy inevitabilmente finisce con il confluire e con il sovrapporsi alla tutela dei consumatori, della concorrenza, a temi legati alla tassazione, alla politica internazionale, alla sicurezza. È ovvio che è un tutt'uno, un magma assolutamente inscindibile. Una di quelle indicazioni che derivano dal famoso studio dell'Organizzazione mondiale per la cooperazione e lo sviluppo è che le *authority* della privacy devono riuscire a collaborare con le autorità antitrust, perché quello che era un tema solo ed esclusivamente legato ai diritti del singolo e

dell'individuo oggi è anche un tema di mercato e senza questo rafforzamento di questa collaborazione la partita non si vince.

Metto in fila, nell'avviarmi alle conclusioni, alcuni suggerimenti, alcune indicazioni, forse solo alcune impressioni.

Al primo posto il tema della cultura: se non restituiamo al cittadino, al consumatore e all'utente, la percezione di quanto vale la sua privacy - come solo un processo culturale lo può fare - la partita è persa, perché se quel diritto ad avere diritti non c'è, come ha scritto più volte Stefano Rodotà, abbiamo delle authority garanti di diritti che i cittadini non sentono neppure di avere.

La consapevolezza del valore della privacy nelle sue molteplici sfaccettature: il valore del dato personale, la riservatezza, l'identità personale.

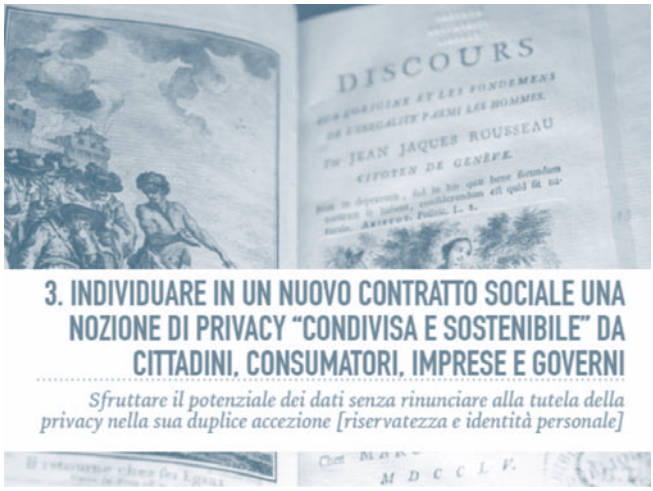
Un altro aspetto che ritengo assolutamente centrale, mi ha fatto piacere sentirlo riecheggiare più volte anche nella sessione precedente, di questa mattina, è che dobbiamo assolutamente fare uno sforzo nel non continuare a ritenere che privacy sia contro qualcosa, contro sicurezza, contro mercato, contro trasparenza e viceversa, cioè che si debba ogni volta scegliere se più mercato, più trasparenza, più sicurezza e meno privacy, da tutte le parti.

Dobbiamo accettare l'idea che stiamo parlando di tessere che appartengono allo stesso identico puzzle. Gli *hashtag* dovrebbero essere "bilanciamento, equilibrio, compromesso", però è ovvio che si deve poter garantire la sicurezza di un Paese, nel rispetto della privacy, si deve poter garantire alle imprese di fare marketing e commercio nel rispetto della disciplina della privacy; si deve evidentemente poter garantire al cittadino di condividere i suoi dati in un contesto che è cambiato.

Quello che secondo me serve è risiglare un nuovo contratto sociale, per dirlo con le parole di Rousseau. Una nozione condivisa di privacy, condivisa da tutti gli stakeholder, condivisa dai cittadini,

dai consumatori, dalle imprese e dai governi; qualcosa che consenta di sfruttare il potenziale, di cui a questo punto siamo tutti convinti, dei dati personali sul mercato, senza rinunciare, evidentemente, alla tutela vera e propria della privacy.

Il segretario generale dell'Organizzazione per la cooperazione e lo sviluppo, nel presentare il famoso studio al quale facevo riferimento prima, dice: "Dobbiamo riuscire a garantire che i benefici di questa *data-driven innovation* siano condivisi, che nessuno resti indietro e che quella che dovrebbe essere un'opportunità di mercato non si trasformi, viceversa, in una ragione di nuovo *"divide"*, di nuova separazione e di nuova ghettizzazione di parte della popolazione.



Vengo poi a quella che era probabilmente la domanda iniziale: l'informativa necessariamente lunga, sotto i quattro, cinque o sei *flag* per l'acquisizione del consenso, è il solo strumento con cui possiamo tutelare la privacy dei singoli nel mercato e nel contesto del quale discutiamo?

Faccio un esempio: un grosso titolare di dati personali pubblica la sua informativa, assolutamente corretta, sotto prevede tre *checkbox* diverse. La prima dice agli utenti: "Vuoi darmi il consenso perché io e le altre società del gruppo possano trattare i tuoi dati personali per finalità commerciali?". La seconda *checkbox* dice: "Presti il consenso a che il titolare del trattamento possa comunicare a soggetti terzi, delle tipologie identificate nell'informativa, i tuoi dati personali per finalità di marketing?". Terza *checkbox*: "Presti il consenso a che noi ti si possa profilare?".

Ebbene, in una verifica che abbiamo fatto di recente quello che viene fuori è che la più parte degli utenti transitati per quelle pagine, parliamo di centinaia di migliaia, hanno messo il *flag* solo sulla voce numero 2, cioè non vogliamo che tu e le tue società del gruppo, di cui pure evidentemente ci fidiamo perché stiamo concludendo un contratto, trattiate i nostri dati personali, ma invece siamo assolutamente favorevole a che tu comunichi i nostri dati personali al resto del mondo.

Naturalmente è un esempio, non pretendo di farne un'indicazione statistica né di ricavarvi degli insegnamenti chissà quanto universalmente validi, però evidentemente quello non è uno strumento di tutela ma è diventato, purtroppo - dico per chi si è occupato prima di consumerismo, che l'ha vissuto in prima persona - niente di più e niente di meno della famosa approvazione specifica delle clausole vessatorie o abusive. Io dico spesso, dopo averne promossa a gran voce l'introduzione, che oggi queste sono il modo più sicuro per l'azienda di porsi al riparo dalla contestazione degli utenti, ma non sono, nel modo più assoluto, il modo più sicuro per l'utente di veder tutelato il suo diritto, in quel caso di consumatore nei confronti dell'azienda.

Alcuni miei modestissimi suggerimenti da lasciare a chi ha questo compito, incredibilmente difficile: prima si diceva che dobbiamo discutere a livello regolamentare solo di modalità con le quali lasciar trattare i dati personali o anche di limiti, io non ho grandi dubbi che in realtà dobbiamo riuscire a riscoprire, dentro questo universo vastissimo che si chiama "diritto alla privacy", un insieme che è un diritto indisponibile dell'uomo.

Ciò che resta fuori da questo micro-insieme deve essere affidato alle regole del mercato: la partita qui è trasparenza, *privacy by design*, le piattaforme usabili, che possono evidentemente fare la differenza, *enforcement* effettivo, e in quest'ambito io credo che la tecnologia non possa davvero mancare, non è una missione umana quella di garantire la privacy di miliardi di connessi, oggi.

Non vorrei aver dato la percezione che siamo di fronte ad una partita che domani mattina vinceremo, so bene che è facile a dirsi ma molto difficile a farsi, credo però che per tutte le cose che ci stiamo dicendo e per quelle che sentiremo dire fra poco il momento per provarci sia davvero ora.

Vi saluto con una frase a me molto cara, di uno scrittore e poeta, Gabriel García Marquez: *"Tutti gli esseri umani hanno tre vite: una pubblica, una privata, una segreta"*. Se le tecnologie riuscissero ad abilitare gli esseri umani a disporre di questi tre livelli, tre profili, probabilmente saremmo tutti quanti un passo avanti.

Grazie.

Giovanna Bianchi Clerici

Grazie all'avvocato Scorza per l'interessantissima prolusione. Le ultime parole mi fanno pensare che se dobbiamo cominciare un po' a ragionare sul possibile superamento del paradigma della informativa-consenso, entriamo in una logica di contesto, dove il contesto in cui si svolge la raccolta, soprattutto l'analisi dei data di questa grande massa di dati, diventa fondamentale. Basti pensare al medesimo dato sanitario: se usato in un certo contesto può dar luogo ad una positiva funzione di utilità sociale, se usato in altro modo può addirittura portare ad una discriminazione.

Il medesimo atto di profilare, con queste sempre più precise, continuamente arricchite, preferenze delle persone, porta inevitabilmente ad un effetto distorsivo perché limita in senso

autoreferenziale le informazioni e i servizi che la rete ci suggerisce, tendenzialmente escludendoci da un elemento in grado di mettere in discussione i nostri convincimenti e le nostre idee consolidate.

Gli americani lo chiamano il fenomeno della filter bubble, della campana di vetro, a cui veniamo sottoposti e, in parte, ci auto-sottoponiamo.

Lancerei adesso questi due spunti al nostro prossimo ospite, che è il dottor Fabio Chiusi, giornalista free-lance, che collabora con importanti testate, fra cui "La Repubblica", "Wired" e "L'Espresso".

È un blogger, "Il Nichilista" e "Chiusi nella rete" sono i blog in cui si esercita. Autore di diverse pubblicazioni, scrive soprattutto di governance, di Internet, censura, dissidenza digitale, analizzando il rapporto assai complesso fra tecnologie digitali, politica e società.

Mi permetto di ricordare anche due pubblicazioni, la più recente è del 2014, "Critica della democrazia digitale. La politica 2.0 alla prova dei fatti" e due saggi sulla retorica dell'odio in rete e sul caso WikiLeaks. Prego.

Fabio Chiusi

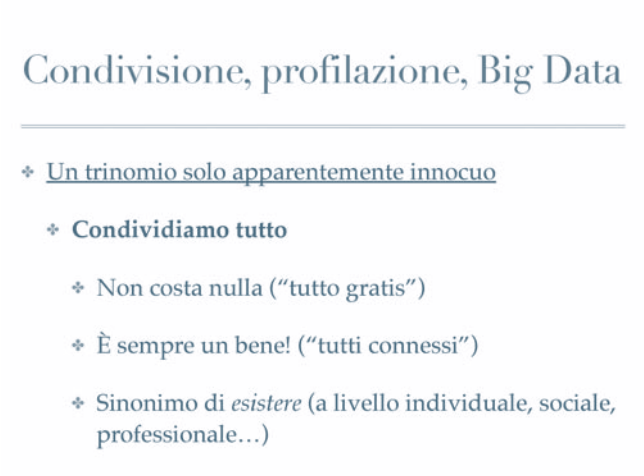
Grazie a tutti per avermi ospitato qui, sono stati veramente dei discorsi stupendi.

In particolare quello del Garante e quello di Spataro mi sono piaciuti molto, vorrei riuscire a prendere il testo di quello che è stato detto e pubblicarlo, perché secondo me sono cose che vanno diffuse e portate fuori da queste stanze, nelle scuole, in mezzo alle persone che poi con la privacy e con i problemi della privacy devono convivere tutti i giorni.

È in quest'ottica pragmatica e un po' anche per non addetti ai lavori che vorrei parlare. Vorrei parlare di una strategia che secondo me - adesso citerò un libro - è molto efficace, per poter provare a difendere la propria privacy on-line, a prescindere dalle soluzione tecnologiche particolarmente complesse e dalle soluzioni

politiche. È una strategia che io ho chiamato "depistaggio", ma che come vedremo si chiama *obfuscation*.

Il punto di partenza è problematizzare il titolo di questo incontro, che per tutti i presenti qui è problematico. Per moltissime persone al di fuori di questa stanza, per chi non ci sta ascoltando, invece non lo è: lo dicono molti sondaggi e lo dimostra anche la reazione al caso Snowden, molto timida dal punto di vista dell'opinione pubblica.



Questo trinomio è solo apparentemente innocuo e vorrei dire perché. Prima di tutto la condivisione secondo me è figlia di una serie di illusioni, che sono addirittura di natura ideologica. Principalmente deriva dal fatto che condividere è considerato, nella nostra era, sempre un gesto positivo, cioè la condivisione on-line viene vista quasi sempre come un fattore positivo, qualcosa che ci rende parte della società interconnessa, ci rende tutti più vicini al prossimo, più tolleranti: tutto questo dovrebbe portare a più democrazia. Abbiamo visto che le cose non sono esattamente così, però fondamentalmente l'ideologia è quella di Mark Zuckerberg, il mondo è connesso. Il mondo probabilmente non va granché bene, ma Zuckerberg sì, perché il suo profitto nell'ultimo trimestre ha superato un miliardo di dollari, per cui sicuramente la sua ideologia a lui fa comodo, probabilmente ai suoi utenti meno.

Tutto questo non costa nulla, perché tutti questi servizi funzionano benissimo ma non costano assolutamente nulla ed è un'altra illusione ideologica, cioè l'idea che sia tutto gratis, quando invece tutti quelli che sono qui in questa sala sanno benissimo che paghiamo con la nostra vita, con i dati personali.

C'è inoltre anche un aspetto esistenziale, che forse è il più triste, cioè che condividere è sinonimo di esistere, di esserci, sia a livello individuale, narcisistico, per dire che ci sono nel momento; sia a livello sociale, per dire agli amici che io ci sono su queste cose, io mi impegno, sono un attivista, mi indigno continuamente; sia a livello professionale perché effettivamente, anche nella mia esperienza di giornalista, se uno è più presente on-line è più facile che arrivi una telefonata da qualche redazione.

La profilazione, ne abbiamo parlato anche nell'introduzione di questo panel: è semplice dire perché la profilazione dovrebbe essere buona, meglio avere una pubblicità che parli proprio a te piuttosto che a uno qualunque; la facilità e la comodità d'uso ne guadagnano, l'esempio più classico sono i discussi cookies, oggetto di una norma altrettanto discussa; i dati poi sono anonimizzati, quindi alla fin fine "di me non si sa molto", questo è quello che si dice, per scoprire che in realtà intrecciando le banche dati sono anonimizzati molto meno.

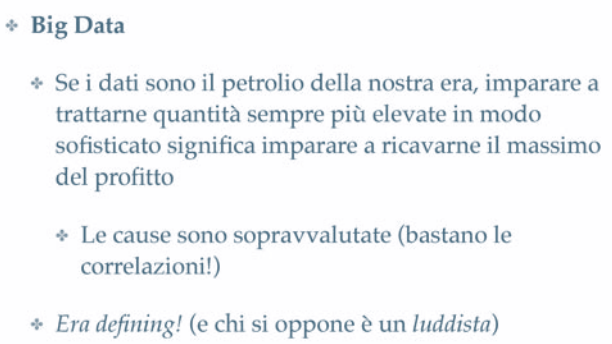
- **Profilazione**
  - Meglio pubblicità personalizzata che generica
  - Facilità/comodità d'uso (es: cookie)
  - I dati sono *anonimizzati*!

"Big Data" è un'altra di quelle splendide parole che non vogliono dire assolutamente nulla ma che piacciono moltissimo a chi deve farci dei soldi, se i dati sono il petrolio della nostra era, imparare a trattarli in quantità sempre più elevate, in modo sempre più sofisticato, significa imparare a ricavarne il massimo del profitto.

Qui c'è anche un aspetto epistemologico, e una cosa mi terrorizza: l'idea che le cause siano sopravvalutate, bastano le correlazioni. Tutto sommato se uno vuole capire quanta acqua deve bere al giorno non serve capire a cosa serve l'acqua, ma basta avere una bottiglia d'acqua con i Big Data che dica "Ora devi bere".

Esiste questa cosa, in commercio: una bottiglia d'acqua che, siccome conosce il tuo fabbisogno energetico, registra qualunque cosa accada nel tuo organismo, ti dice quanto dovresti bere e quando. Non siamo nemmeno più liberi di bere un sorso d'acqua, senza che ce lo dica un computer.

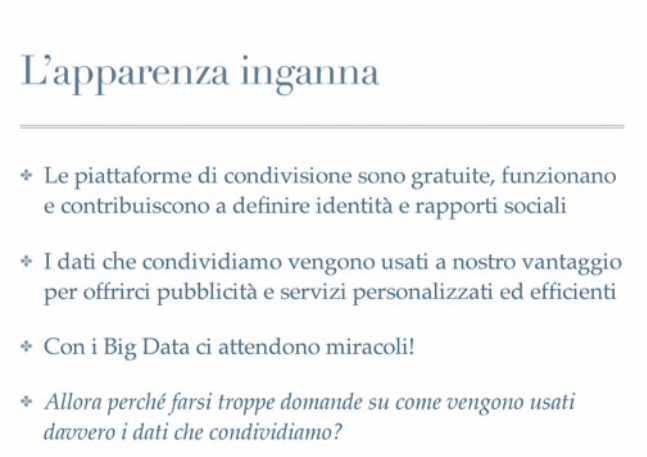
Cosa si potrebbe opporre a quello che definisce la nostra era, l'era dei Biga Data? "Sei un luddista!", salvo poi scoprire che i luddisti non erano dei cattivissimi antiprogressisti e conservatori, ma erano delle persone che avevano a cuore i diritti dei lavoratori e non volevano che non fossero travolti dall'era delle macchine, cosa che è dannatamente attuale, peraltro; ma questa è un'altra operazione di finzione ideologica, secondo me.



Abbiamo scoperto che tutte queste apparenze ingannano.

Come abbiamo detto le piattaforme di condivisione sono gratuite, i dati che condividiamo servono a darci servizi più efficienti, i Big Data ci porteranno a fare miracoli, ci attendono miracoli con questa era magnifica dei Big Data, quindi perché farsi troppe domande?

Questa è la domanda che mi viene posta molto spesso quando scrivo di queste cose, questo è il *feedback* che ricevo molto spesso, da giornalista. Perché farsi troppe domande: da chi vengono usati i nostri dati, chi li tratta e con chi li condividiamo? Dopotutto abbiamo sentito che le spie spiano, se non fai niente di male non c'è nulla da temere.



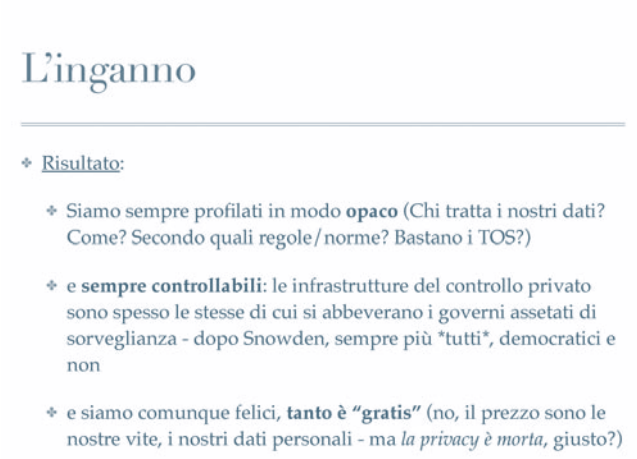
L'avvocato Scorza ha citato il nostro beniamino Zuckerberg che dice che la privacy fondamentalmente è morta. Casualmente tutti questi grossi soggetti delle multinazionali riescono ad avere queste splendide idee, che poi finiscono per portarci a meno democrazia e meno diritti per tutti.

Il risultato è l'esatto opposto, naturalmente: siamo sempre profilati in modo opaco, non sappiamo bene chi tratta i nostri dati, speriamo che con la nuova normativa europea lo si possa sapere meglio.

Bastano davvero i termini e le condizioni di utilizzo per capire queste cose? No, abbiamo scoperto anche che siamo

diventati tutti soggetti sperimentali, siamo tutti criceti che girano nella ruota di Facebook, basta che Facebook alteri un pochino la velocità della ruota e si alterano le emozioni. Se uno era depresso perché ha visto più post negativi o che causano emozioni negative sul feed, è una cosa che agli ingegneri dei dati di Facebook non interessa particolarmente.

Siamo anche sempre controllabili, altro piccolo dettaglio, per cui si scopre che queste aziende danno accesso diretto ai loro server, almeno questo diceva Snowden, ai governi, che così possono essere sempre più informati su cosa facciamo, magari in maniera automatica, visto che ormai sono gli algoritmi a decidere chi è un terrorista, molto spesso. Anche in Francia lo si è visto e in Italia è un'idea che piace molto. Inoltre siamo tutti felici, perché tanto è tutto gratis. Naturalmente il problema è che la realtà è opposta.

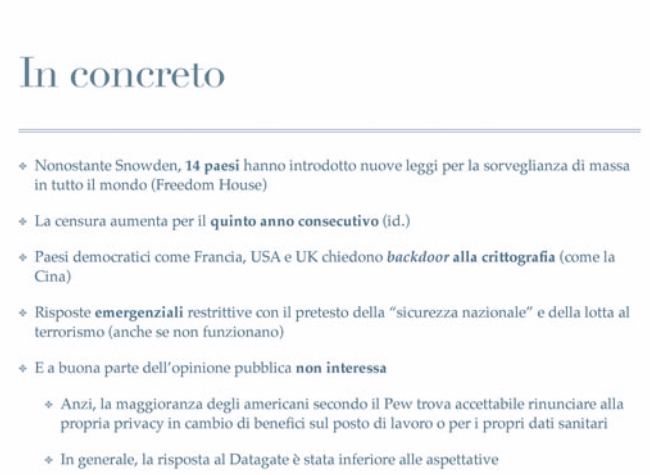


Abbiamo visto che *Freedom House* nell'ultimo rapporto dice che 14 Paesi nel mondo hanno introdotto nuove leggi sulla sorveglianza di massa, nonostante Snowden, in quest'ultimo anno; che la censura aumenta per il quinto anno consecutivo; che si ricomincia a parlare - ed è tristissimo - di *backdoor* e crittografia.

Nonostante sia un dibattito che si era risolto nella metà degli anni '90, queste cose continuano a venire fuori e a rendere

più insicura la rete per tutti, per provare a prendere più terroristi, che è una cosa completamente folle; risposte emergenziali, che sono altrettanto folli di solito - e per fortuna abbiamo sentito qui il senatore Minniti dire che non c'è questa intenzione da parte del governo italiano, per adesso non ce n'è traccia, per fortuna.

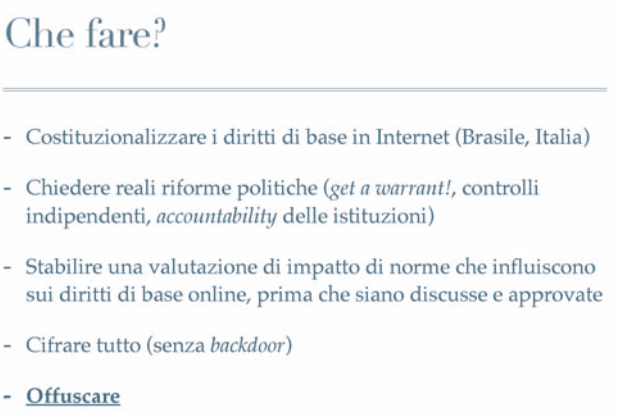
Abbiamo scoperto anche che a buona parte dell'opinione pubblica tutto questo non interessa e questa è una cosa che io vi posso testimoniare, scrivendo per molte testate, provando ad avere a che fare con le persone su Internet, sentendone i feedback: questa cosa è veramente diffusa.



Cosa possiamo fare? Qui viene in campo l'aspetto più pratico, secondo me. Ci sono varie soluzioni: costituzionalizzare alcuni diritti di base, che è un punto di partenza e da questo punto di vista l'Italia finalmente è un modello per il mondo insieme al Brasile ed è una buona cosa; si possono chiedere reali riforme politiche, facciamo in modo che ci sia un passaggio dalla magistratura, che ci siano controlli indipendenti, che le istituzioni siano responsabili, cioè che ci sia *accountability*, anche se abbiamo visto in questi giorni che le bozze del Freedom of Information Act italiano - lo dico incidentalmente, l'abbiamo pubblicato ieri su Valigia Blu - non ci consente di dire che effettivamente alla propaganda corrispondono poi i fatti.

Un'altra idea che era circolata era stabilire una valutazione di impatto di queste norme che influiscono su Internet, ma che in realtà influiscono sulla vita di tutti, sempre, non soltanto quando siamo on-line: anche questa potrebbe essere un'idea, dire "non continuate a riproporre le stesse norme, che non hanno alcun significato da vent'anni, proviamo invece a fare un passo oltre e diciamo perché queste norme non hanno significato, facciamone un database, facciamo in modo che i politici che non hanno familiarità con questa cosa possano avere immediatamente un deposito, dove per esempio scoprire quali sono le conseguenze di alcune cose che dicono". Io temo lo ignorino e questo è un problema.

Si può anche avere una risposta tecnologica, cioè cifrare tutto, è una delle soluzioni che storicamente, dalla fine degli anni '90, alcuni movimenti di attivismo su Internet hanno cercato di portare avanti e che in parte anche Snowden, Assange e altri attivisti contemporanei dicono. Cifrare tutto è comunque sempre un bene, in un contesto del genere.



La soluzione di cui vorrei parlare brevemente è "offuscare", cioè spezzare la pericolosità del trinomio di cui stiamo parlando, perché il pericolo di questo trinomio deriva dal fatto che la condivisione, la profilazione e i Big Data parlino esattamente di noi, cioè che siano esatti, che producano delle profilazioni

che raggiungono noi, i nostri gusti, li anticipino e li ingabbino, in un certo senso.

Il problema della *filter bubble*, di cui si parlava prima, è che noi finiamo per diventare vittima della nostra stessa propaganda: molto spesso finiamo per essere esposti solamente a opinioni che sono congruenti alla nostra, perché un algoritmo vuole che sia così, perché sa che ci piace. Io per esempio uso molto l'algoritmo di Spotify, quando ascolto musica. Per un certo periodo Spotify mi ha fatto scoprire delle cose, poiché andava sempre più nel dettaglio di alcuni generi musicali che io gli fornivo, dopodiché è arrivato al limite del dettaglio e a un certo punto non aveva più niente da dirmi, ha cominciato a propormi musica piuttosto dimenticabile perché non aveva più idea di cosa propormi, aveva esaurito il ventaglio.

Il problema è con tutto il resto della musica finisce per propormi magari un cantautore di quarta categoria invece di Jobim, perché magari non sa che mi piace la musica brasiliana e ignora un gigante. Questo fanno questi algoritmi. Che cosa succede se noi invece proviamo a confondere le tracce, se proviamo a dire delle cose sbagliate su noi stessi agli algoritmi che ci tracciano? Questo è interessante, secondo me.

L'offuscamento

- Il trinomio condivisione-profilazione-Big Data regge **come pericolo** finché è esatto, personale, riguarda proprio ciascuno di noi
- Che accade quando invece confondiamo le nostre tracce, e il tracciamento finisce per riguardare una persona che in realtà **non esiste**?

Qui c'è un manuale che viene chiamato *"User's guide for privacy and protest"*, che si chiama *"Obfuscation"*. È un manuale

molto breve, agile, bello, pubblicato pochi mesi fa, i cui autori sono Finn Brunton e Helen Nissenbaum.

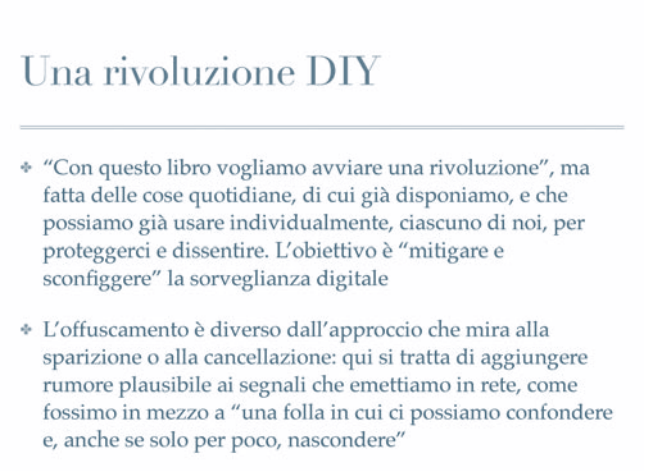
Definiscono l'offuscamento in questo modo: "L'offuscamento, nella sua definizione più astratta, è la produzione di rumore modellato su segnali esistenti, così da rendere la raccolta dei nostri dati più ambigua, confusa, difficile da sfruttare e manipolare; e, da ultimo, ridurne il valore".

È un'idea che non nasce certo con Internet, è un'idea che le persone che protestano mettono in atto con mezzi molto poveri, da sempre, ma che si può applicare tranquillamente al tracciamento su Internet. "

Si tratta di avviare una rivoluzione - dicono gli autori, ma è una rivoluzione povera, fatta di cose quotidiane, di ciò di cui già disponiamo e che possiamo già usare individualmente, è una cosa che possiamo fare da questo istante - per proteggerci e dissentire. L'obiettivo è mitigare e sconfiggere la sorveglianza digitale, sapendo che l'efficacia dipende molto dal contesto, dipende molto da cosa vogliamo ottenere e non è una strategia esatta", naturalmente. Si tratta di provare a mettere in campo varie strategie di cui adesso diremo brevemente.

È importante sottolineare che l'offuscamento è diverso dall'approccio che mira a sparire da Internet, a cancellare le

proprie tracce, per esempio, è una soluzione che consente di dire che non devi chiudere Facebook per non essere tracciato, per esempio, è un'obiezione antiluddista, se proprio vogliamo usare questi termini.

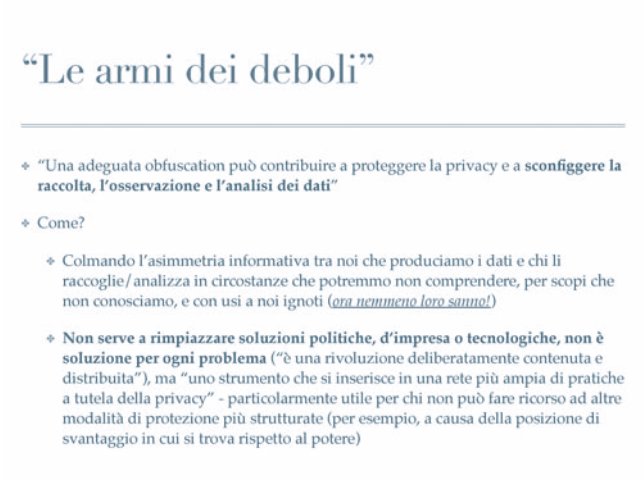


Secondo me non è una buona idea disconnettersi da Internet o andare contro Internet, perché Internet è una macchina della sorveglianza. La macchina della sorveglianza si può inceppare, piuttosto, si può "fregare" in qualche modo. "Si tratta quindi di aggiungere rumore plausibile ai segnali che mettiamo in rete, come fossero in mezzo a una folla in cui ci possiamo confondere e, anche solo per poco, nascondere".

Qui si tratta quindi di contribuire, come dicevo, "a sconfiggere la raccolta, l'osservazione e l'analisi dei dati, colmando in una certa misura l'asimmetria informativa tra noi che produciamo i dati, che non sappiamo come vengono trattati, e chi li raccoglie, che invece lo sa benissimo", sono parole del libro.

Con questa tecnica si potrebbe dire "ora nemmeno voi lo sapete", questo è un po' il punto.

Naturalmente tutto questo sempre sapendo che non serve a rimpiazzare soluzioni politiche, soluzioni commerciali, soluzioni tecnologiche, non è una soluzione perfetta; infatti si parla di una rivoluzione deliberatamente contenuta e distribuita.

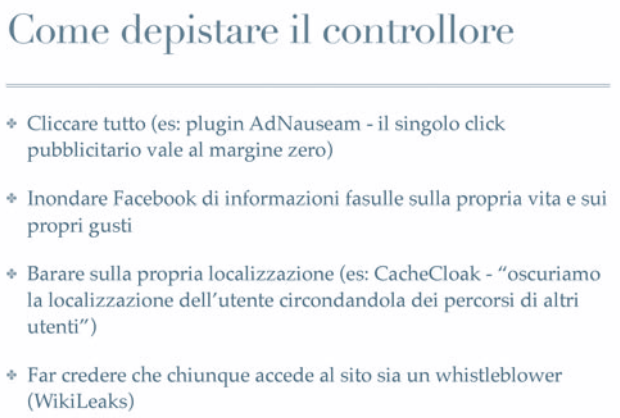


È particolarmente utile per chi non può fare ricorso ad altro. Se per esempio uno non ha competenze particolari che gli consentano di usare PGP o altri strumenti di crittografia forte, per esempio, o magari in un Paese dove la crittografia addirittura è vietata o ostacolata, si può comunque ricorrere a questi metodi.

Ad esempio, una di queste modalità per depistare il controllore è cliccare tutto, naturalmente a proprio rischio e pericolo, perché si possono prendere malware e spam di ogni tipo, però se si prendono delle valide protezioni ci sono dei plug-in che consentono di cliccare ogni singolo banner pubblicitario, che a questo punto comincia a valere a margine zero.

Si può inondare Facebook di informazioni fasulle sulla propria vita e i propri gusti, si può cominciare a cliccare "mi piace" su cose che non piacciono, si può cominciare a dire che si è stati tre volte in India quando non ci si è andati, si può cominciare a dire cose di qualunque tipo. È stato fatto da varie persone e in effetti la vita che ne risultava era assolutamente impossibile per qualunque essere umano. Ma l'algoritmo di Facebook non è un essere umano e quindi per lui era assolutamente plausibile. Si può barare sulla propria localizzazione, che è un'altra cosa importante, visto che i dati di localizzazione spesso possono dire molto delle nostre vite personali; e c'è anche chi come WikiLeaks, ad esempio, ha usato delle strategie, in questo

caso tecniche, non più semplici. È un'altra modalità per far capire che questa cosa è fattibile e funziona, anche a livello tecnico: ad ogni persona che accedeva al sito veniva iniettato un codice per cui sembrava che stesse postando del contenuto, di modo che a questo punto non si sapeva bene chi era che stava pubblicando del contenuto sui canali di WikiLeaks. A quel punto è molto più difficile individuare un possibile *whistleblower* nella folla.



Questa è l'ultima conclusione ed è il modo con cui vorrei lasciare un messaggio di speranza, che prescinde da soluzioni politiche, tecnologiche o di altro tipo. Dicono gli autori: "In situazioni in cui non si può dire no, restano le opportunità per un coro di inutilissimi sì e questi inutilissimi sì potrebbero aiutare a salvare la privacy".

Grazie.

Giovanna Bianchi Clerici

Grazie, dottor Chiusi. Prometto che leggerò assolutamente questo libretto, perché sicuramente è un punto di vista molto particolare. Tra l'altro leggevo proprio qualche giorno fa che una giornalista, credo canadese, ha cercato di nascondere la propria gravidanza alla rete ricorrendo ad una serie di stratagemmi, anche

abbastanza complicati, perché voleva verificare la possibilità di farlo, visto che ha scoperto che una donna incinta per la rete vale 2 dollari al giorno!

Chiuderemo questa sessione con il professor Maurizio Ferraris, ordinario di Filosofia teoretica presso la Facoltà di Lettere e Filosofia dell'Università di Torino. Dirige, nella medesima Università, il Centro interuniversitario di Ontologia teorica e applicata e il laboratorio di Ontologia. Direttore della rivista di estetica fino al 2010, ha collaborato con il supplemento cultura del Sole 24 Ore, ora scrive per le pagine culturali di Repubblica e conduce un programma su Rai 5, *"Lo stato dell'arte"*, dove si affrontano temi di attualità, politica e cultura. Ha scritto moltissimi libri, più di 50: ricordiamo *"Il manifesto del nuovo realismo"* del 2012 e *"Mobilitazione totale"* dello scorso anno.

Professore, lo spunto è questo: la nostra identità soggettiva sotto questa tempesta di dati come cambia? Possiamo ancora parlare in senso stretto di dato personale e fino a che punto possiamo tollerare questa asimmetria di potere, che è stata poco fa molto precisamente descritta, fra chi detiene i dati e chi li fornisce, purtroppo spesso in maniera anche inconsapevole?

Maurizio Ferraris
Privacy, sicurezza, emergenza

Come cambiano le nostre idee di privacy, di sicurezza e di segretezza ai tempi dei social network? Non credo che l'essere umano abbia mai avuto un'idea precisa riguardo ai concetti di privacy o di segretezza. Mark Zuckerberg, il fondatore di Facebook, è in fondo un ottimista se sostiene che di colpo il tema privacy non importi più; probabilmente se iniziamo a porci seriamente la questione, il problema tornerà a essere centrale.

Guido Scorza ha ricordato quella massima secondo cui esisterebbero tre vite: quella pubblica, quella privata e quella segreta. Eppure nel Seicento Samuel Pepys ha scritto un libro intitolato

"La mia vita segreta", annotando ogni minimo particolare della sua vita – una vita di cui adesso sappiamo tutto. La sua vita, allora, è la meno segreta che si possa immaginare, e questo perché Pepys era un grafomane. Fosse vissuto ai giorni nostri, avrebbe di certo faticato meno: il mezzo-internet avrebbe fatto la sua gioia, perché avrebbe reso il suo autoesibizionismo totale e continuativo

È su questo punto che vorrei soffermarmi. Talvolta, come ha sottolineato Fabio Chiusi, sarebbe necessario rendersi invisibili.

Ma quanti seguono o seguiranno realmente questo consiglio?

Qualcuno di sicuro, ma probabilmente la maggior parte non lo farà: non credo, infatti, che l'umanità sia libertaria e liberale. Spesso, anzi, quando si confronta il nostro stile di vita con altre forme di civilizzazione che consideriamo diverse – e magari anche inferiori, per esempio quando si dice che l'Islam vuole privarci della nostra libertà – emerge il fatto che la libertà, non intesa come valore ispiratore di un sistema politico, ma come tendenza umana, non è ciò che sorregge le democrazie occidentali.

Si è spesso parlato, riferendosi al Web, di servitù volontaria. Non dobbiamo però dimenticare che Alexis de Tocqueville, scrivendo *"La democrazia in America"* affermava che una delle caratteristiche della democrazia in America è la servitù tranquilla, dolce, volontaria del suo popolo.

Sono anch'io convinto del fatto che la democrazia sia un bene irrinunciabile; spesso però avviene questo: ci si illude di possedere una innata tendenza alla democrazia, cioè di essere nati liberi e desiderosi a tutti i costi di continuare a esserlo, salvo poi diventare, per qualche perversa tendenza, sottomessi a qualcuno o a qualcosa (e così avviene per esempio che la protezione dei nostri dati personali non è più ritenuta fondamentale).

L'animale umano è in realtà un animale più sottomesso e docile di quanto si possa pensare. Il libro di Michel Houellebecq, *"Sottomissione"*, è molto indicativo riguardo a questo punto. Lo scrittore ci mette di fronte a questo scenario: improvvisamente Parigi assiste a un cambiamento politico, la classe intellettuale della

città – professori, intellettuali laici, ecc. – si convince ben presto della convenienza di avere più mogli e accetta i valori della nuova classe dominante. In che modo possono avvenire trasformazioni sociali di questa natura? È proprio su questo punto che vorrei ora focalizzare l'attenzione.

La libertà o la privacy non sono qualcosa di dato una volta per tutte, ma qualcosa che dobbiamo conquistarci e preservare continuamente. Ad esempio, in questo momento ho al polso un apparecchio di alta tecnologia che mi dice "alzati", perché conta i miei passi e cerca in questo modo di incentivare il mio dimagrimento. Sono io ad aver acquistato questo sofisticato apparecchio, nessuno mi ha imposto di indossare questo oggetto che, a rigore, assomiglia agli strumenti di controllo che si utilizzavano per controllare i carcerati. L'ho comprato io ed è per questo che non affermo che gli altri sono asserviti laddove io sarei libero.

Faccio un altro esempio. Una notte fra il sabato e la domenica mi sono svegliato, ho guardato il telefonino per vedere che ora fosse e ho constatato che era arrivata una mail di lavoro. Automaticamente ho cominciato a rispondere: stavo lavorando alle 3 di notte, in una notte fra il sabato e la domenica. Era, di nuovo, una mia scelta, nessuno mi costringeva a farlo. Dobbiamo fare i conti con questa caratteristica dell'essere umano.

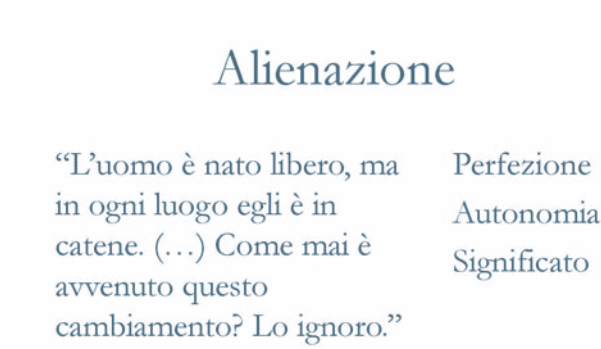
Quando dico che "l'animale è mobilitato" parlo essenzialmente di quell'animale che sono io: e però si può notare una specie di allegoria, perché in questo caso si vede un tipo di animale incatenato in maniera visibile, nel senso che è costretto a un laccio evidente, laddove l'altro animale è legato a un laccio meno evidente, ma non meno forte. Oltretutto quell'animale il laccio se l'è trovato, mentre l'altro ce l'ha per sua volontà. Non sto criticando quell'animale, che poi sono io, che risponde alla mail alle 3 di notte e si è preso quest'altro laccio. Dico semplicemente che bisognerebbe partire proprio da questo dato antropologico.

I. L'animale mobilitato

Siamo abituati a pensare che l'essere umano sia libero e che aspiri per natura alla libertà e che poi, per qualche forma di alienazione, cambi, diventi diverso da quello che è. Tutte le valutazioni che si fanno sul Web portano a farci esclamare: "come ci siamo ridotti!"; ci si dimentica però come si era prima. Io credo che la tecnologia, più che alienazione sia rivelazione, ci mostra cioè quello che siamo. Inoltre la tecnologia ha una seconda utilità. Infatti ci mostra che non è necessario arrivare a postulare teorie del complotto o teorie paranoiche per cui c'è una grande mente che ci sta sfruttando: essenzialmente queste cose non sono costruite,

ma emergono di per sé. Le compagnie telefoniche non avevano pensato, quando hanno introdotto gli SMS, che la macchina per parlare sarebbe diventata una macchina per scrivere, dunque per registrare, dunque per esporre molto di più i nostri dati. Invece gli umani hanno preferito la scrittura alla voce, gli *scripta manent* ai *verba volant*. Questo è un dato, non c'è neanche bisogno di trascrivere se si vuole controllare qualcuno, l'SMS è più comodo e più compatto. Se si sta spiando qualcuno, è utile che questi mandi un SMS, che è un'informazione breve, concisa e già trascritta. Se invece si dovesse fare come nel film *"Le vite degli altri"*, come nella Berlino Est dove affittavano un appartamento al piano di sopra per ascoltare quanto avveniva sotto, ci troveremmo in un gioco senza fine[1].

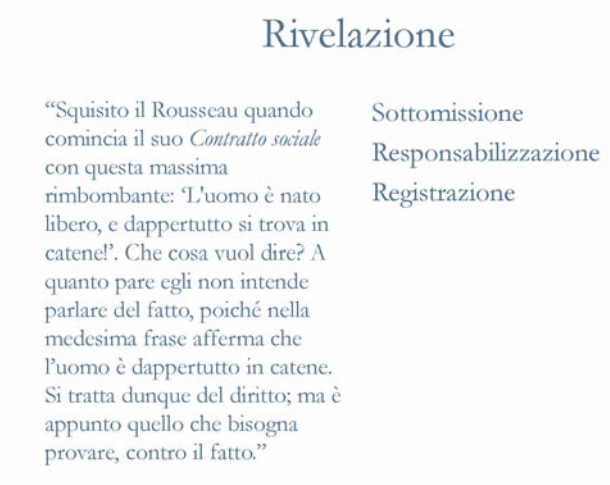
II. Alienazione e Rivelazione



Riprendiamo tutta la questione con ordine: l'alienazione. Rousseau ha questa idea, veramente bizzarra, per la quale: "L'uomo è nato libero, ma in ogni luogo è in catene". Alla celeberrima frase il filosofo aggiunge: "Come è avvenuto questo cambiamento lo ignoro". È già bello di per sé ritenere che l'uomo sia nato libero, ancor meglio è credere che dopo, non si sa bene come, sia caduto in ogni luogo in catene. Tuttavia l'ipotesi ha un merito, ossia quello

(1) Per inciso, uno dei motivi del crollo economico della DDR era la necessità di dover mantenere tutte quelle spie. Un quarto della popolazione faceva la spia, ma qualcuno, a Berlino, avrà pur dovuto produrre qualcosa, nel frattempo.

di porre una semplice domanda: "sarà vero che è libero?". Ad ogni modo Rousseau avrebbe almeno dovuto spiegarci come sarebbe caduto in catene. Invece non lo spiega, perché sullo sfondo del suo ragionamento vi è l'idea che l'essere umano, che nasce perfetto, autonomamente dotato di significato, sia in seguito stato rovinato dalla tecnica. Quest'idea ritorna in tutto ciò che si legge e si dice riguardo a Internet: della gente che guarda solo i telefonini, che non parla più alle feste di Natale perché sta guardando il telefonino, come se si trattasse di un'alienazione: no, è semplicemente l'apparizione di ciò che noi siamo. Io direi che, piuttosto, abbiamo una rivelazione.



Fra l'altro un pensatore conservatore, Joseph De Maistre, affermava: "Squisito Rousseau quando comincia il suo contratto sociale con questa massima rimbombante: l'uomo è libero e dappertutto si trova in catene. Che cosa vuol dire? A quanto pare egli non intende parlare del fatto, poiché nella medesima frase afferma che l'uomo è dappertutto in catene. Si tratta dunque del diritto, appunto quello che bisogna provare contro il fatto". Io credo, contrariamente a quello che conclude De Maistre, che è favorevole al diritto divino e alla sottomissione, che noi dobbiamo provare, contro il fatto (nello specifico, il fatto che l'uomo non sia libero per natura) il diritto alla libertà che possediamo. Però è la necessità di provare contro il fatto che ci

dimostra la tendenza fortissima dell'umano alla sottomissione, alla responsabilizzazione.

III. Emergenza

Perché si è passati dal parlare allo scrivere? Perché è attraverso questo passaggio che si ricevono degli ordini. La spunta su *Whatsapp*, che dimostra che hai letto il messaggio, rende il destinatario in qualche modo responsabile: l'ordine è arrivato a destinazione e tu non rispondi. Pensate ai tempi remoti e felici in cui si usciva di casa alle 8 di mattina, e in casa cominciava a squillare il telefono, che continuava ancora per 12 ore, fino al ritorno del proprietario di casa che, se non aveva attivato la segreteria telefonica, non era responsabile in alcun modo di alcunché. Non era responsabile perché nulla era stato registrato: tutte le chiamate arrivate andavano perse e con esse anche il loro ricordo.

Non si tratta dunque soltanto di rivelare i propri dati, ma anche di mettersi in una condizione di responsabilità, di debito nei confronti di messaggi che ci arrivano. Se uno guardasse la televisione e pensasse che lo speaker si sta rivolgendo a lui, proprio a lui, sarebbe probabilmente uno schizofrenico. Se invece sei sul Web, effettivamente ci si sta proprio rivolgendo a te e molto spesso sei chiamato a rispondere.

Hegel ha insegnato che gli esseri umani vogliono essere riconosciuti, ma del resto anche senza Hegel ci saremmo arrivati. Contemporaneamente si evidenziava il fatto che, pur di essere riconosciuti, gli esseri umani sono disposti a rinunciare alla loro privacy. Tengono in maggior conto il fatto che gli altri sappiano di loro rispetto agli svantaggi che derivano dal rivelare se stessi.

Banalmente, tutto quello che viene scritto e registrato, per esempio ciò che sto scrivendo ora, resterà per l'eternità, molto più di quanto non si verificava un tempo. Siamo arrivati alla situazione paradossale per cui tutti potenzialmente potrebbero sapere dove tu sia ora che stai telefonando; cosa questa che invece non avviene mai nei rapporti interpersonali non mediati da apparati tecnologici.

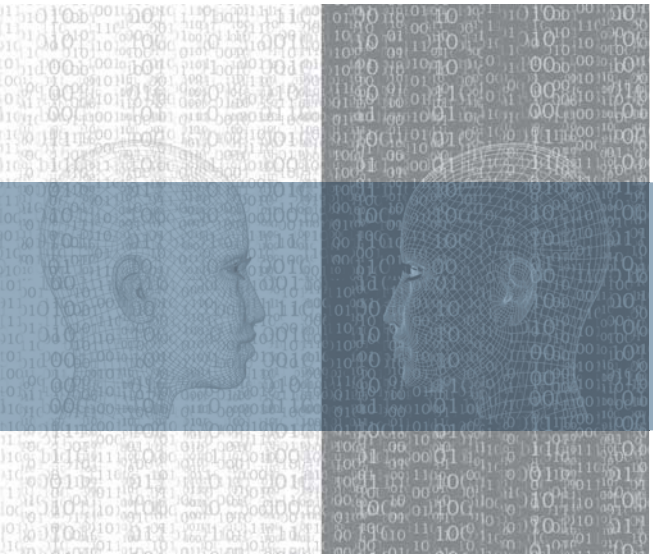
Tuttavia, perché parlo di "emergenza"? In fondo abbiamo scoperto qualcosa che non può essere giustificato attraverso elementi utilitaristici, per esempio. Cosa spingesse le persone ad andare in fabbrica, un tempo, era abbastanza evidente, ed era il fatto che le persone avevano bisogno di guadagnare. Che cosa spinga un individuo a rispondere nella notte fra le 2 e le 3 del sabato, è molto meno chiaro. Questo è un elemento che fa parte della natura dell'essere umano.

Aristotele ha detto che l'uomo è un animale dotato di linguaggio, ed effettivamente gli sviluppi degli apparati tecnologici lo dimostrano. Non aveva però immaginato un animale così sottomesso, proprio perché non disponeva di esempi così lampanti.

Questa enorme sottomissione, che caratterizza la rivoluzione informatica, che fra l'altro è stata immaginata inizialmente come una grandissima liberazione, non va vista come una condanna per la natura umana, ma, al contrario, deve stimolarci per ragionare sul fatto che l'uomo non è naturalmente libero. La riflessione sulla privacy deve andare nella direzione della liberazione della natura umana. L'aver scoperto che l'uomo è intrinsecamente dipendente-da potrebbe essere un vantaggio, non so se filantropico o altro, che probabilmente non sarebbe mai emerso se non avessimo dovuto far fronte a questo genere di problemi.

Giovanna Bianchi Clerici

Grazie, professore. L'ultima sessione è quella coordinata dalla professoressa Licia Califano.



Privacy e sicurezza nella società digitale

Sessione III

Gian Domenico Caiazza
Avvocato

Carlo Nordio
Magistrato

Stefania Maurizi
Giornalista

Moderatore **Licia Califano**
Componente del Garante
per la protezione dei dati personali

Sessione III

Privacy e sicurezza nella società digitale

Licia Califano

L'intensificazione della minaccia terroristica negli ultimi mesi, a partire dalla strage di Parigi del 13 novembre scorso, ha naturalmente portato i governi, le organizzazioni sovranazionali e l'opinione pubblica di tutto il mondo a interrogarsi sulle misure più idonee ad assicurare la sicurezza e l'integrità delle persone e degli Stati.

Di fronte a episodi così scioccanti per l'immane violenza delle azioni e l'indistinzione degli obiettivi, la risposta che emerge con maggiore forza consiste perlopiù nell'inasprimento delle misure di polizia e nell'intensificazione delle attività di prevenzione.

Ciò, peraltro, consapevoli che l'attuale minaccia di attentati terroristici ha determinato un arretramento della garanzia dei diritti umani e delle libertà destinato a durare nel tempo e socialmente percepito quale inevitabile conseguenza del pericolo prevalente.

Si tratta di uno scenario che impone la ricerca di principi e criteri direttivi per la definizione di regole in grado di contemperare le esigenze di difesa della incolumità personale con le irrinunciabili esigenze di difesa dei diritti e delle libertà fondamentali: dal diritto alla riservatezza al diritto alla protezione dei dati personali, dalla libertà di circolazione a quella di domicilio.

Un bilanciamento che inevitabilmente riapre la discussione, per il vero mai chiusa, del rapporto fra difesa dell'ordine e della sicurezza pubblica e garanzia delle libertà civili.

Non voglio entrare nella questione della configurabilità di un diritto alla sicurezza idoneo a contrapporsi, nel bilanciamento,

ai diritti di libertà. Più opportunamente si può considerare la sicurezza quale scopo che può giustificare misure restrittive della libertà. Sicurezza, in questa lettura, quale ragione dinamica di limiti ai diritti riconosciuti, in definitiva implicitamente deducibile dalla nostra Costituzione.

Il problema che si pone è quindi quali siano le misure accettabili, tenendo ben presente che un conto è la percezione sociale del bisogno di sicurezza, ed un conto sono le valutazioni strettamente giuridiche.

Quanto alle risposte concrete che stanno affiorando, ecco alcuni recenti esempi noti a tutti:

- l'Unione europea sta per giungere all'approvazione del Pnr (*Passenger name record*), un enorme database contenente i dati di tutti coloro che salgono su voli aerei per i quali partenza e/o destinazione si trovi all'interno del territorio europeo, che potrebbe essere messo a disposizione del Dipartimento Usa per la sicurezza nazionale;

- la Francia ha prolungato il ricorso a misure restrittive eccezionali (come le perquisizioni domiciliari in assenza di controllo giudiziario o lo scioglimento delle associazioni sospette), ma l'intenzione è quella di portare la disciplina dello stato di emergenza direttamente in Costituzione; non dobbiamo dimenticare che queste decisioni hanno recentemente scatenato ripercussioni politiche importanti sullo stesso governo francese;

- in Inghilterra il Parlamento si sta concentrando sull'*Investigatory powers bill* che, nella sua attuale formulazione, tra le altre cose consentirebbe alle forze dell'ordine e di sicurezza di acquisire e conservare per un anno i dati sui siti internet visitati da parte di tutti gli utenti, nonché di procedere a massicce operazioni di intercettazione telefonica e telematica, il tutto con la collaborazione coatta di compagnie telefoniche e fornitori di comunicazioni elettroniche.

Si noti che tutte le misure di sorveglianza e repressione

attualmente in discussione hanno l'effetto di limitare contestualmente due diritti fondamentali che spesso si trovano in reciproca contrapposizione, ossia il diritto alla privacy e la libertà di manifestazione del pensiero: anche questi due diritti finiscono così per condividere la sorte di "vittime" indirette del terrorismo.

Ciò detto, non dobbiamo dimenticare che la nostra è una democrazia anche perché si fonda sull'inviolabilità dei diritti e delle libertà fondamentali, quali forme di espressione della dignità umana; le nostre democrazie non possono arretrare né snaturarsi a fronte di una minaccia terroristica. E non dobbiamo dimenticare che l'esperienza del terrorismo che colpì l'Italia negli anni '70 è stato vinto senza bisogno di snaturare il sistema democratico.

La stessa impostazione metodologica è seguita anche dalle Corti di Lussemburgo e Strasburgo nel loro ruolo di custodi dei diritti, e in questa veste ricordano all'Europa che essa stessa è, prima ancora che obiettivo privilegiato dei terroristi, la regione del globo più avanzata in termini di cultura dei diritti. Oggi sono le Corti europee a porre argini a tutela del diritto alla protezione dei dati personali dalle non necessarie e sproporzionate invasioni poste in essere attraverso decisioni politiche e scelte normative.

La Corte di giustizia dell'Unione europea negli ultimi anni ha licenziato due sentenze storiche: quella dell'aprile 2014 sulla *data retention*, in base alla quale la legislazione comunitaria sull'accesso ai dati di traffico telefonico e telematico da parte delle forze di pubblica sicurezza, tra le altre cose, si fondava su una conservazione indifferenziata e generalizzata dei dati, anche in termini di durata temporale, e non subordinava tale accesso a precisi presupposti sostanziali e procedurali; quella di fine 2015 che ha invalidato l'accordo *Safe Harbour* del 2000 tra Commissione europea e Usa, proprio perché le autorità statunitensi potevano acquisire in maniera massiccia e indiscriminata, e per esigenze di sicurezza nazionale, i milioni di dati personali di cittadini europei archiviati presso i server delle tante società americane che dominano il mercato mondiale dei servizi legati a internet.

Ma è di due settimane fa una pronuncia della Corte europea dei diritti dell'uomo che sembra rispondere proprio alle sollecitazioni di stampo securitario di queste ultime settimane (caso Szabó e Vissy c. Ungheria, deciso il 12 gennaio 2016, n. 37138/14).

Essa ha ad oggetto una legge antiterrorismo ungherese del 2011, che, pur nel riconoscimento di una generale ammissibilità di forme di sorveglianza segreta per finalità antiterrorismo, viene pesantemente censurata dal giudice dei diritti in quanto introduceva incisivi poteri di perquisizione, registrazione e intercettazione delle comunicazioni elettroniche, senza dall'altra parte contemplare forme sufficientemente precise, effettive e comprensibili di garanzia per gli interessati; si tenga presente che anche il giudizio di costituzionalità interno si era rivelato severo.

Queste le misure contestate: 1) la sottoposizione a sorveglianza segreta di ogni persona che si trovi in Ungheria, in assenza di una previa definizione delle categorie di individui potenzialmente sospettabili; 2) la richiesta, da parte della task force antiterrorismo, di autorizzare le intercettazioni, in assenza di una prova dell'evidenza della loro effettiva necessità e con il potere dispositivo nelle mani esclusive del Governo (nella specie, il Ministro della Giustizia); 3) la possibilità che la sorveglianza, di base limitata a 90 giorni, potesse venire prorogata di fatto più e più volte; 4) la totale assenza di controllo giudiziario sull'autorizzazione al ricorso alla sorveglianza, quale fonte di possibili abusi da parte dell'esecutivo; 5) la completa inefficacia delle forme di controllo parlamentare sulla predetta attività dell'esecutivo.

In altre parole, con riferimento al trattamento dei dati personali, la Corte di Strasburgo mostra come, anche di fronte alla legittima esigenza di rafforzare la sicurezza e prevenzione, occorre sempre tenere in adeguata considerazione i principi di necessità, finalità, proporzionalità e temporaneità.

A questo punto, vorrei chiedere ai nostri relatori se la legittima definizione di misure di prevenzione, investigazione, accertamento e repressione dei reati contro le nostre democrazie

debba per forza condurre alla silenziosa accettazione di qualsiasi forma di restrizione dei nostri spazi materiali e giuridici di vita.

Il ciclico oscillamento del pendolo verso esigenze di controllo della società e dei consociati deve arrivare necessariamente a comprimere il diritto alla protezione della nostra sfera privata e personale e la libertà di espressione del nostro pensiero oltre il confine del contenuto essenziale del diritto? Venendo poi alle specifiche misure il ricorso massiccio alle intercettazioni telefoniche e telematiche è giustificato sul piano degli effettivi risultati o produce non necessarie e sproporzionate limitazioni al nostro diritto alla privacy?

Ne parliamo con Gian Domenico Caiazza, avvocato penalista del foro di Roma, Carlo Nordio, attualmente procuratore aggiunto presso il Tribunale di Venezia, e Stefania Maurizi, giornalista d'inchiesta che collabora con l'Espresso.

Gian Domenico Caiazza:

Ringrazio il Presidente Soro per questo invito, che credo abbia avuto il senso, per quanto riguarda la mia persona, di dare voce al punto di vista dell'avvocato penalista da un osservatorio privilegiato, che è quello del processo penale, sui delicatissimi temi qui in discussione.

"Privilegiato" nel senso che il processo penale è forse il luogo elettivo nel quale si misura con pienezza lo scontro tra esigenze di sicurezza della collettività, vale a dire esigenze di prevenzione e di repressione dei reati, e i fondamentali diritti di libertà della persona.

Esiste una regola dello Stato di diritto, che non può mai essere derogata: se momenti particolari della vita sociale e politica di un Paese possono giustificare misure straordinarie per ("accertamento e la repressione delle attività illecite, questa cultura della eccezionalità non può mai riguardare il processo penale, cioè il momento nel quale gli elementi raccolti nel corso delle indagini

e delle investigazioni devono essere vagliati sotto il profilo della loro legittimità e quindi sotto il profilo del rispetto dei diritti di rango costituzionale dei soggetti che in quel momento sono imputati.

Quel giudizio deve sempre e comunque rispettare le sue regole ordinarie, a prescindere dalla qualità dell'imputato, dalla gravità del reato contestato, dall'allarme sociale che esso provoca in quel preciso momento storico.

Ma anche gli strumenti investigativi, dunque i mezzi di ricerca della prova, devono in ogni caso arrestare la propria forza invasiva della sfera di libertà, riservatezza e dignità della persona entro i limiti invalicabili fissati dalla carta Costituzionale.

Ed invece, la storia giudiziaria e giurisprudenziale degli ultimi anni - dovremmo dire decenni - mostra di essere tendenzialmente recalcitrante all'idea del rigoroso rispetto di quei limiti, sia nell'uso degli strumenti investigativi, sia nel modellare in concreto i limiti di ammissibilità e legittimità della prova penale così in concreto raccolta.

Il tema delle intercettazioni, dunque dell'ascolto o comunque della captazione delle comunicazioni riservate (telefoniche, informatiche, ambientali) tra persone, è dunque inevitabilmente il luogo naturale di scontro tra esigenza di sicurezza della collettività e diritti inviolabili della persona.

Ora, è difficilmente controvertibile che, dal punto di vista strettamente normativo, le intercettazioni telefoniche, ambientali o dei flussi informatici siano lo strumento investigativo presidiato dal maggior numero di garanzie in favore dell'indagato. Norme processuali alla mano, disporre un'intercettazione di conversazioni riservate tra persone è senza dubbio alcuno l'atto più complesso e più sottoposto a verifiche di legittimità e di utilizzabilità probatoria, addirittura superiori a quelle che presidiano la privazione cautelare della libertà personale.

E purtuttavia la storia delle intercettazioni in questo Paese è una storia frequente di abuso di questo strumento, perché si può

presidiare con ogni possibile attenzione normativa l'uso di uno strumento così invasivo, ma se l'atteggiamento direi culturale che ne accompagna l'uso è quello di privilegiare in ogni modo la sua micidiale efficacia invasiva nella ricerca della prova, è inesorabile che le norme di rigore e di garanzia saranno piegate a questo obiettivo.

Ecco allora che i provvedimenti che le autorizzano sono quasi sempre fondati su motivazioni stereotipe e solo apparenti; che esse non si fondano, di fatto, sulla preventiva rilevazione di gravi e concreti indizi di reato in corso di commissione, ma sono - assai spesso - finalizzate esse stesse alla ricerca di indizi di reato; che il limite ordinario di quindici giorni viene regolarmente derogato; che viene puntualmente elusa l'udienza stralcio, pur prevista dal legislatore come immediatamente successiva al deposito delle intercettazione, dove il GIP, sentite le parti, dovrà stralciare ed eliminare dal circuito processuale tutte le conversazioni irrilevanti ai fini del processo, o assunte in modo illegittimo; e potremmo continuare negli esempi.

Ciò che più preoccupa è che queste costanti tensioni giurisprudenziali volte in concreto a favorire e legittimare un uso sempre più invasivo e meno rigoroso dello strumento intercettativo, si sviluppano su di un terreno pure massimamente presidiato a livello Costituzionale, dove la tutela del diritto alla segretezza della corrispondenza ed alla inviolabilità del domicilio approntata dagli artt. 14 e 15 della Costituzione è tale da riservare solo alla legge le eccezionali ipotesi della loro limitazione.

Non è allora difficile comprendere come e perché la giurisprudenza penale si senta ancora più libera nell'uso e nella legittimazione di atti investigativi e di ricerca della prova chiamati a misurarsi con un presidio costituzionalmente più debole quale è quello di cui gode il c.d. diritto alla riservatezza, costituzionalmente radicato nell'art. 2 della Costituzione, e dunque nel generale catalogo dei diritti della personalità, non assistito da riserva di legge.

Esemplare, in questo senso, la sentenza delle SS.UU. della Corte di Cassazione n.7 del 28 marzo 2006, ricorrente Prisco, chiamata a dare una soluzione sistematica ed univoca al tema della captazione di immagini nel domicilio privato ed in luoghi diversi da esso, ma riservati (il privè di un night club, una toilette pubblica, et similia).

Ebbene, quella sentenza ha stabilito, nell'ordine, che: a) le immagini c.d. "non comunicative" video-captate nel domicilio private sono radicalmente illegittime perché inderogabilmente vietate dal precetto costituzionale (della inviolabilità del domicilio); b) che le videoriprese di comunicazioni "comunicative" (si pensi alla gestualità comunicativa tra due persone) nel domicilio privato debbano assimilarsi in toto alle intercettazioni di comunicazioni, e dunque sono ammissibili alle rigorose condizioni normative che regolano quelle (art. 266 e segg. C.p.p.); c) le videoregistrazioni effettuate in luoghi comunque riservati ma diversi dal domicilio privato, misurandosi - per quanto prima ricordato - con un livello affievolito di tutela costituzionale, possono dunque essere disposte addirittura dal Pubblico Ministero in fase di indagini, con un provvedimento motivato ma sottratto a provvedimenti autorizzativi giurisdizionali.

Ancora più allarmante, d'altronde, è quello che sta per accadere, che è già accaduto e che temo soprattutto accadrà riguardo alle cosiddette perquisizioni informatiche, uno strumento investigativo di frontiera, indiscutibilmente micidiale: si invia da remoto un software, che si installa, a mia insaputa, sul mio computer e da quel momento ogni volta che il mio computer entra in collegamento con la rete esso sarà monitorato, dalla digitazione della tastiera ai siti che frequento, ai documenti che scrivo.

La giurisprudenza si è già misurata con questi strumenti, e le prime decisioni sono tutt'altro che incoraggianti, perché confermano una pregiudiziale indisponibilità a privilegiare la tutela dei diritti fondamentali di libertà della persona rispetto all'uso di strumenti investigativi così performanti.

Occorre riconoscere la complessità delle problematiche poste dall'uso investigativo di questi software. Si tratta di mezzi di ricerca della prova che contengono tracce tipiche di altri mezzi regolati dal nostro codice, senza tuttavia identificarsi pienamente in nessuno di essi. Non sono infatti tecnicamente assimilabili né alla perquisizione, né alla ispezione, pur assomigliandovi, per la semplice ragione che, diversamente da quelle, vengono disposti ed effettuati all'insaputa del destinatario; si avvicinano di più alle intercettazioni dei flussi informatici, senonché queste ultime hanno ad oggetto flussi comunicativi bi-direzionali (mail, chat, etc.), non la comunicazione unidirezionale dell'utente con il proprio hard disk (frequentazione di siti, redazione di documenti, etc.).

La quinta sezione penale della Corte di Cassazione (sentenza n. 1813 del 14.10.2009, Virruso ed altri), respinse il ricorso proposto dagli imputati che chiedevano dichiararsi la inutilizzabilità di tutte le prove acquisite da un "captatore informatico" installato segretamente sui computer degli indagati.

La Corte ha escluso potersi qualificare l'uso di quel trojan alla stregua di una intercettazione informatica effettuata dunque senza autorizzazione del Giudice e perciò illegittima; e ciò in base alla considerazione che con quello strumento non si erano intercettati flussi comunicativi tra due soggetti colloquianti, ma dati documentali già formatisi e comunque frutto di rapporto univoco tra l'utente ed il proprio computer. Legittimamente dunque il PM aveva disposto l'acquisizione informatica (e ovviamente segreta) di quei dati con provvedimento motivato ex art. 234 c.p.p., cioè alla stregua di acquisizione motivata di documenti. Una decisione davvero sorprendente, considerata la micidiale invasività della sfera privatissima dell'indagato operata dunque senza nemmeno il vaglio preventivo ed autorizzativo del Giudice.

E' facile immaginare la tumultuosa evoluzione di questi strumenti investigativi, destinati ad implementare la propria micidiale invasività, senza alcun freno o limitazione da parte del giudice di legittimità.

E' dunque evidente la necessità, ormai improcrastinabile, di una nuova definizione dei beni costituzionali in gioco, magari muovendo verso la definizione - suggerita dalla dottrina più avvertita - di una nozione di "domicilio informatico" quale evoluzione della tradizionale nozione di domicilio definita e protetta dall'art. 14 della Costituzione. Pensare di potersi affidare alla elaborazione giurisprudenziale di rigorosi principi di tutela del diritto alla riservatezza, da opporre alla crescente, devastante invasività dei nuovi strumenti informatici di investigazione, non ci porterebbe lontano.

Si trattava di questo, dell'installazione di un trojan, la difesa ha detto che era stato disposto semplicemente con un decreto motivato del pubblico ministero, di acquisizione di documenti, ex articolo 234, senza perder tempo in tecnicismi. Si dice che non c'è bisogno di una richiesta di autorizzazione, non è un'intercettazione. La difesa insorge dicendo che questa è un'attività intercettativa micidiale. Tra l'altro questo *trojan* è rimasto lì per otto mesi.

La Corte di Cassazione conferma il provvedimento del tribunale del riesame, che rigetta l'eccezione dicendo che è correttamente un'acquisizione di documenti, perché non si è intercettato un flusso comunicativo tra due soggetti. Se ci sono due soggetti, se io sto parlando, o chattando con qualcuno, questa è un'intercettazione, ma "noi siamo andati a prendere i documenti che si sono formati e che si formano durante quegli otto mesi".

È legittimo, il decreto, qualora il provvedimento abbia riguardato l'estrapolazione di dati non aventi ad oggetto un flusso di comunicazioni già formati e contenuti nella memoria del personal computer o che in futuro sarebbero stati memorizzati. Si ritiene quindi legittimo non solo entrare, a mia insaputa, sul mio computer, e prendere come un documento i miei file, ma anche prendere quelli che formerò nel corso del tempo.

Cosa c'è alla base di una giurisprudenza del genere, di un'idea del genere? In realtà qui è in discussione un bene,

un diritto, il diritto alla riservatezza, che è un diritto, sì, di rango costituzionale, ma meno rafforzato di quello del domicilio o della segretezza della corrispondenza, perché nasce dall'articolo 2 della Costituzione, non è tutelato da un'esplicita riserva di legge, quindi si dice che è un diritto costituzionale, sì, ma per essere compresso non richiede le forme solenni che richiedono le intercettazioni telefoniche.

Qui ci sono due considerazioni da fare: una è quella di un dato culturale, cioè il nostro è il processo ispirato al principio del *male captum bene retentum*, cioè come li ho presi non ha importanza, una volta che li ho presi, ed è un po' quello che connota, su questo tipo di tematiche, la nostra giurisprudenza e la nostra riflessione, anche con testimonianze giurisprudenziali importanti.

Ricordo la sentenza delle Sezioni unite sul tema della captazione delle immagini domiciliari e nei luoghi riservati e la distinzione che fa quella sentenza, pregevolissima, peraltro.

Se vogliamo avere chiari i ragionamenti che si fanno su questi temi cruciali, basta leggere la sentenza delle Sezioni unite che dice, meno male, che l'intercettazione di immagini nel domicilio privato è *ab origine* illegittima se, però, le immagini sono non comunicative, cosa che comincia già ad essere un problema. Cioè, se invece io riprendo le immagini di due persone, a casa di una delle due, che stanno parlando fra di loro, dicono le Sezioni unite, non è altro che un diverso modo di documentare un'intercettazione colloquiale e quindi è legittimo. Se invece io riprendo immagini non comunicative, cosa che faccio a casa mia, allora qui c'è una nullità originaria, c'è un'incostituzionalità.

Cosa succede, invece, perché il caso lo poneva, se devo intercettare in una toilette pubblica, in questo caso era il privè una discoteca? Qui la cosa è diversa, perché sono zone riservate - vedete l'idea del diritto alla riservatezza come un diritto minore rispetto al domicilio - ma non garantite dal divieto originario, che gli articoli 14 e 15 della Costituzione pongono rispetto al domicilio

e quindi con i provvedimenti minimi dell'Autorità Giudiziaria.

Questo ha aperto riflessioni dottrinarie e giurisprudenziali importanti, nel senso che occorre che il diritto alla riservatezza acquisisca un riconoscimento di maggior forza all'articolo 8 CEDU, che aiuta in questo senso a togliere il diritto alla riservatezza da quest'ambito di diritto costituzionale minore; se così fosse, le conclusioni sarebbero, in ordine alla perquisizione informatica, che essa può essere disposta solo nelle forme autorizzative delle intercettazioni e, naturalmente, alle condizioni che lì sono regolate.

A me pare che dal fronte del processo penale non giungano buone notizie, in termini di questo forte rispetto dei diritti costituzionali che sono messi in discussione da questo scontro cruciale tra esigenze di sicurezza e processo.

Mi auguro che riflessioni come queste, così belle e interessanti, che stiamo sviluppando qui e che io sto ascoltando, ci aiutino a crescere in questo senso, nel senso di una forza sempre maggiore delle libertà della persona.

Carlo Nordio

Grazie per l'attenzione. L'intervento aveva un abstract, che forse vi è stato distribuito: esso riguarda proprio la disciplina delle intercettazioni telefoniche e ambientali, che peraltro, nella sua forma patologica, è già stata ben descritta negli interventi precedenti.

Non posso però esimermi dalla prima domanda che ha posto la nostra coordinatrice, con delle considerazioni che, oltre a essere giuridiche, sono per metà filosofiche e per metà storiche: esse riguardano il rapporto tra sicurezza e libertà.

Si tratta di una relazione tra vasi comunicanti: quando aumenta la sicurezza la libertà diminuisce, e quando aumenta la libertà può diminuire la sicurezza. La Giustizia sta come schiacciata nel mezzo. Ma quale valore viene prima?

La risposta è una sola. La sicurezza prevale sulla libertà e anche sulla Giustizia. Possiamo constatarlo osservando la storia: uno Stato può esistere senza libertà ma non senza sicurezza. Stati sicuri, ma non liberi, purtroppo ne abbiamo visti tanti, nella dittatura sovietica, nella dittatura nazista, nella dittatura fascista.

Erano Stati senza libertà ma che sono sopravvissuti e per un certo periodo hanno anche prosperato. Se non fosse intervenuta la guerra sarebbero durati anche di più. Perché uno Stato, purtroppo, può sopravvivere senza libertà, se è sicuro, ma uno Stato non può vivere senza sicurezza, perché senza di essa vi è un'anarchia, vi è un ricorso al fai-da-te della giustizia, oltre che all'autotutela.

Nell'ordine logico, politico e filosofico, quindi, mi duole dirlo come liberale, la sicurezza prevale.

Questo concetto, però, non deve costituire un alibi per eliminare le libertà fondamentali, al di fuori di quei casi sporadici, rari, per fortuna, in cui la sicurezza dello Stato è messa in pericolo. Giustamente questa mattina il collega Spataro ha sottolineato che noi abbiamo avuto il privilegio di indagare più di trent'anni fa sul fenomeno delle brigate rosse, di Prima Linea e delle varie organizzazioni terroristiche. Io ho portato a processo la colonna veneta, e il collega Spataro quella di Milano. Il nostro orgoglio è stato quello di aver debellato questo perniciosissimo attentato allo Stato, rispettando la legge, rispettando le leggi dello Stato e magari suggerendo al legislatore delle leggi nuove, che fossero però in perfetta armonia con la nostra Costituzione.

Questo è un altro punto di orgoglio della magistratura italiana della nostra storia.

State tuttavia sicuri che se il fenomeno brigatista fosse andato oltre, superando i limiti della tolleranza, probabilmente saremmo arrivati alle leggi speciali. Non esistono tabù ideologici quando è in pericolo la sicurezza dello Stato.

La stessa pena di morte, che oggi fa inorridire qualsiasi persona di buon senso, non è poi così stravagante, se si pensa che Mussolini è stato condannato a morte e che la sentenza è stata

eseguita. Ci sono delle circostanze, nella storia di un Paese, in cui anche la pena di morte può intervenire. Prima della Costituzione repubblicana, ma dopo la fine della seconda guerra mondiale, la pena di morte, come ben sapete, è stata applicata ed è stata eseguita, in Italia.

Fatta quindi una *tabula rasa* di questi tabù, la domanda è: la situazione attuale legittima o no la riduzione delle nostre libertà fondamentali? Io sono profondamente convinto di no. Allo stato attuale non vi è alibi, non vi è legittimazione per vulnerare i diritti individuali. Fra questi individuali fondamentali io metto il diritto costituzionalmente protetto dall'articolo 15 della Costituzione, della libertà e della riservatezza delle comunicazioni interpersonali.

La riservatezza è l'interfaccia della libertà di manifestazione del pensiero.

Questa mattina sono stati citati molti filosofi, abbiamo sentito di Rousseau, di Kant e di altri. Permettetemi di citare Pascal, che sosteneva che se tutti sapessero quello che noi diciamo degli altri, non avremmo più un amico, e quindi non saremmo liberi. Perché, aggiungo io, le parole che spesso pronunciamo al telefono, a casa, o altrove, sono frutto proprio di equivoci personali, sono delle deiezioni scabrose del nostro intelletto e delle nostre passioni, di cui poi magari ci pentiamo; ma una volta che sono state tradotte, scritte, riportate nei brogliacci telefonici e magari sui giornali, rimangono per l'eternità. Ci troviamo di fronte a un colossale strumento invasivo, che va dunque gestito e maneggiato con estrema prudenza.

Lo fa il codice di procedura penale? Certamente lo fa. Lo fa così bene che ha appuntito la matita fino a spezzarla.

La disciplina del codice di procedura penale è infatti chiarissima: i brogliacci della Polizia giudiziaria non hanno nessuna validità e non hanno nessuna credibilità: devono di conseguenza essere trascritti nelle forme della perizia attraverso un contraddittorio davanti a un giudice terzo, previa selezione della difesa e dell'accusa, ognuna delle quali deve individuare le parti che le interessano.

È buono e giusto che sia così. Perché quando io dispongo di un'intercettazione telefonica o ambientale, posso fare quello che diceva Richelieu: "datemi una lettera e una forbice e io farò impiccare il suo autore". Facciamo un esempio. Io parlo di polvere bianca con il mio interlocutore telefonico e poi dico che quella polvere bianca mi ha attenuato il bruciore di stomaco.

Bene se la Polizia giudiziaria, senza manipolare l'intercettazione, porta al magistrato solo la prima parte di quella intercettazione, tutti penseranno che stia parlando di cocaina. Non c'è una manipolazione dell'intercettazione, ma attraverso una selezione arbitraria si dà, della verità, una rappresentazione ingannevole.

La selezione che viene fatta prima, dalla Polizia giudiziaria o dallo stesso magistrato, è già la prima perversione – nel senso proprio di deviazione - dell'articolo 15 della Costituzione.

La seconda è che in queste intercettazioni, così come vengono portate all'attenzione del PM, prima di essere periziate - ammesso che lo siano, ma non lo sono quasi mai - manca la cosa più importante, cioè il tono.

Il tono di voce, quando due persone parlano, è così fondamentale che nel mio amatissimo Veneto, dove non vi è la capacità espressiva e la ricchezza di linguaggio, la tavolozza lessicale, che magari hanno i romani o i siciliani, ma vi è una certa difficoltà nell'espressione, molto spesso la parolaccia e la bestemmia surrogano il contenuto della frase. Tant'è vero che ci siamo trovati di fronte, qualche volta, ad una trascrizione, in questi brogliacci di PG, della frase blasfema. Qualche volta è indicata la divinità offesa, in altri casi si arriva alla specificazione della "bestemmia (affermativa)". Questo perché dal tono di voce si capisce che quella bestemmia è un "sì". Ma esistono le parolacce interlocutorie, esistono le parolacce negative, quelle che esprimono disappunto, sgomento o sorpresa. In conclusione, se io non sento il tono della voce non riesco a capire quale sia la vera volontà, il vero intendimento di chi mi parla.

Un'altra patologia è che la libertà di stampa o, meglio, il diritto delle persone a essere informate sui fatti, è un'altra mistificazione colossale, che non c'entra nulla con la diffusione delle conversazioni captate. Quando il giornalista, ricevendo queste veline dal magistrato, dall'avvocato, dal cancelliere, dal carabiniere o dalla guardia di finanza, insomma, da chi le ha in mano, le riporta, si trova nella stessa situazione in cui vi trovate voi quando, ammesso che lo facciate, guardate "Un giorno in pretura" o quelle trasmissioni giudiziarie che vengono riprese attraverso la sapiente manipolazione del regista.

Quando guardate questi film, non vedete quello che volete voi, come fareste assistendo a un processo normale. Voi in realtà guardate quello che vuole il regista, e non siete affatto liberi di scegliere. Se il regista vuole mandare un messaggio subliminale, per esempio di inaffidabilità, inquadrerà le mani sudaticce del testimone che gesticolano mentre parla. Allo stesso modo chi legge le intercettazioni telefoniche e ambientali nei giornali non legge tutta la verità, legge quello che il giornalista, la prima vittima di questa mistificazione, ha ricevuto, previa selezione di chi gliele ha date. Il giornalista non le ha scelte fra una marea di informazioni che sono utili per la diffusione della verità, fa solo il passacarte di chi gli ha dato le informazioni. Costui, a sua volta, divulgherà quelle utili alla sua causa. Sfavorevoli o favorevoli all'indagato a seconda che la manina appartenga all'inquirente o al difensore.

L'alibi della cosiddetta libertà d'informazione e del diritto alla cronaca non regge dunque a una minima valutazione critica.

Ultima considerazione: molto spesso l'intercettazione coinvolge persone che non c'entrano assolutamente nulla con la chiacchierata dei due interlocutori. Questi terzi sono senza difesa.

Se Tizio parla con Caio è già molto problematico risalire alla vera volontà di Tizio e Caio, perché, come abbiamo detto, può essere manipolata, perché manca il tono, perché non è integrale, eccetera. Ma se Tizio e Caio parlano di Sempronio, Sempronio non può farci nulla. E se Tizio e Caio sono dei delinquenti, e spesso lo

sono, sono anche molto prudenti, per non dire astuti e maliziosi.

Presumendo di essere intercettati, se vogliono vulnerare l'onore di una persona, cosa fanno? Parleranno di lui. Questa terza persona si vedrà sbattuta sui giornali, con il famoso titolo "Spunta il nome dell'onorevole Tal dei Tali", semplicemente perché Tizio e Caio, parlando fra di loro e magari sapendo di essere intercettati, hanno voluto "delegittimare" - uso malvolentieri questo neologismo che non mi piace - questa terza persona, che magari è un ministro o un politico. Il quale dovrà difendersi da una questione che non lo riguarda, magari perché è stata assolutamente inventata, o maliziosamente creata.

Questo è accaduto a tutti, a Presidenti della Repubblica, ex Presidenti della Repubblica, ex Presidenti del Consiglio. Manca soltanto il Papa, e non è detto che un giorno non ci arrivi, visto che il nostro Pontefice usa spesso il telefono.

Cosa fare, allora?

Ci sono due sistemi attraverso i quali le intercettazioni arrivano ai giornali. Uno è illegittimo, quando il giornalista, in un modo o nell'altro, riesce a carpirle, ancor prima che vengano depositate agli atti. Per fortuna sono fenomeni più rari, anche se avvengono. Una volta ad esempio, nel famoso processo "Abbiamo una banca", sono stati condannati i giornalisti proprio perché la bobina non era nemmeno stata consegnata al Pubblico Ministero.

Molto spesso invece avvengono in modo legittimo, perché il Pubblico Ministero le inserisce nelle richieste di ordinanza di custodia cautelare e il Gip le recepisce nel momento in cui emette il provvedimento. Infine il fascicolo finisce al tribunale della libertà, che legge tutto, così come leggono avvocati, interpreti, segretari, e, inevitabilmente i giornalisti.

Si noti che la scelta del Pubblico Ministero di depositare queste intercettazioni è virtualmente insindacabile. E d'altro canto PM e Gip, volendo, potranno trovare una motivazione anche per l'inserimento di un rapporto sessuale in un'intercettazione

telefonica e ambientale. Ci sarà sempre un modo di sostenere che anche quei sospiri di passione avevano una valenza nelle indagini e quindi era utile inserirli. Ecco come, in modo assolutamente legittimo, le intimità delle persone vengono squadernate al pubblico ludibrio.

La soluzione? Ripiegare sulle intercettazioni preventive.

Esse vengono sempre decise dall'Autorità giudiziaria, ma restano nella cassaforte dell'Ufficio, nella massima segretezza, sotto la responsabilità del magistrato e dell'ufficiale di PG che le gestisce.

Badate bene, le intercettazioni preventive non sono mai finite sui giornali, né possono finirci, proprio perché non entrano nel fascicolo processuale.

Se io dunque dovessi dare un modestissimo suggerimento direi di ridurre al minimo le intercettazioni che vengono considerate oggi come mezzo di prova o come mezzo di ricerca della prova; e di ampliare, invece, anche al di là dei limiti di oggi, quelle che si chiamano cosiddette intercettazioni preventive.

Esse valgono come spunto di indagine, esattamente come sono le confidenze della Polizia. Sono utilissime, anche se non valgono come prova. Del resto raramente, alla fine, i testi delle intercettazioni resistono come prova al vaglio dibattimentale.

Esse tuttavia consentono di avere una vastissima visione, sia dei fenomeni terroristici, sia dei fenomeni mafiosi, sia dei fenomeni di corruzione e un domani, Dio non voglia, di un terrorismo internazionale. Grazie.

Stefania Maurizi

Buongiorno, ringrazio l'Autorità garante per l'invito a parlare.

Non sarà un *dulcis in fundo*, non ci sarà dolcezza, perché io non vedo dolcezza nella realtà che dobbiamo esaminare. Io vedo, anzi, un convitato di pietra in questo convegno: parliamo ancora di libertà, di libertà di stampa e la libertà di stampa non c'è se

non c'è la tutela delle fonti, nessuno parlerà mai più con noi se non ha la certezza di essere tutelato, di non essere ascoltato, seguito, eccetera. Tutto questo possiamo dire che è morto, è un romantico ricordo, perché viviamo nella società della sorveglianza di massa.

E questa non è una paranoia, a tre anni dalla pubblicazione dei primi file di Edward Snowden noi abbiamo una certezza, un dato di fatto: il dato di fatto è che esiste una società, un'azienda, che in realtà è un apparato dello Stato, degli Stati Uniti, che si chiama *"National Security Agency"* (Nsa) e che è stata descritta dal prestigioso magazine americano *New Yorker*, come la più potente, la più costosa e la più tecnologicamente sofisticata agenzia di intelligence del mondo, che ha materialmente, realmente, la capacità tecnica di intercettare le conversazioni e i dati dell'intero pianeta.

Questa non è una distopia che noi immaginiamo, non è il frutto di una paranoia, di una teoria della cospirazione - teorie per le quali non ho alcuna simpatia - è un dato di fatto, provato nero su bianco dai file di Snowden. Posso dirlo per averci lavorato, per averli portati in Italia, abbiamo letto questi documenti top secret, che sono il frutto del sacrificio di una fonte, Snowden appunto, che poi racconteremo. Quando tutti noi li abbiamo presi in mano, a nostro rischio e pericolo e a rischio e pericolo della fonte, siamo rimasti senza parole, ci siamo detti "è vero che si possono intercettare le conversazioni dell'intero pianeta?". Sì, è vero, per tre ragioni.

Innanzitutto la fattibilità tecnica: la tecnica ha superato tutto. Fattibilità tecnica ed economica si sono saldate e hanno reso possibile intercettare e sorvegliare l'intero pianeta. Nello Utah, gli Stati Uniti stanno costruendo una struttura che raccoglierà le conversazioni di tutto il pianeta per i prossimi cento anni. Non solo le conversazioni, ma anche tutti i dati bancari, le carte di credito, i dati sanitari e quelli dei voli degli abitanti di tutto il pianeta. Tutto questo - e ci tengo a sottolineare questo aspetto- non è un cascame, un sottoprodotto, dell'era digitale in cui noi

ci siamo ritrovati: è il frutto di una scelta politica precisa, presa dopo l'11 settembre. Come si sono scelte le torture, si è scelta la sorveglianza di massa, che è frutto di leggi approvate nel segreto.

Non le avremmo scoperte se non fossero usciti i file di Snowden.

Magari avremmo potuto immaginarle, ma nessuno di noi avrebbe letto di queste decisioni politiche, esplicitate nero su bianco.

Questa situazione è il frutto di una decisione politica precisa, in cui siamo finiti, senza alcun dibattito pubblico e senza alcun consenso pubblico, che mi risulti.

Se vogliamo fornire dei dati concreti: *"Prism"* è uno dei tanti, delle decine di programmi di sorveglianza di massa, che ha creato la Nsa. Cosa fa Prism? Accede direttamente ai server dei giganti digitali, come Yahoo, Facebook, Google, Apple, e prende tutto: post, conversazioni, conversazioni Skype, eccetera. O anche *"Tempora"*: un altro dei tanti programmi di sorveglianza. È stato messo a punto dal Gchq che è il gemello inglese della Nsa, che si considera superiore alla Nsa, tanto è vero che l'ex capo del Gchq ha detto: "gli americani hanno i soldi, noi abbiamo i cervelli", questa è la loro concezione. Il programma Tempora succhia direttamente dai cavi sottomarini a fibra ottica, che sono le grandi autostrade delle comunicazioni digitali, e prende tutto: telefonate, post su Facebook, i video che guardate, la navigazione internet. Nel 2012, secondo i file di Snowden, il Gchq collaborando con la Nsa, era in grado di intercettare 600 milioni di telefonate al giorno con il programma Tempora. Anche questo, come Prism, è solo uno dei tanti programmi di sorveglianza di massa operati dalla Nsa con il Gchq.

Non voglio polemizzare con il dottor Marco Minniti, ma lui oggi ha dichiarato, davanti a tutti, che in Italia non c'è raccolta massiva di dati. Avendo pubblicato i documenti top secret di Edward Snowden su l'Espresso e su Repubblica - i giornali per cui lavoro - con il collega Glenn Greenwald, ed essendo questi

documenti pubblici, per l'Italia possiamo dire che questi file, fra le altre cose, dimostrano che dal 10 dicembre 2012 al 9 gennaio 2013 la Nsa ha intercettato i metadati di 45.893.570 telefonate degli italiani.

I metadati sembrano una banalità: voi direte: sì, la Nsa ha raccolto i metadati, ma non ha preso il contenuto delle conversazioni, perché i metadati comprendono "solo" le informazioni: chi chiama chi al telefono o chi contatta chi per email, a che ora lo contatta, da dove e quanto dura la conversazione telefonica, se si tratta di un contatto telefonico e a che ora avviene lo scambio email se si tratta di posta elettronica. Questi dati sembrano poco rilevanti, perché in fondo non includono il contenuto della conversazione. In realtà, non lo sono affatto, però, ormai per capire cosa avviene nella vita di una persona, non c'è neanche più bisogno del contenuto delle sue conversazioni: se avete miliardi di metadati di un certo individuo – e la Nsa ha miliardi di miliardi per ciascuno di noi- non serve neanche più sapere cosa dice al telefono quella persona, perché nel caso della sorveglianza Nsa ci muoviamo su un'altra scala, che non è quella del procuratore che ha bisogno del contenuto di una conversazione intercettata.

Incrociando solo i metadati, miliardi di metadati, facendo data mining, profilazione, è possibile sapere tutto di un individuo, senza bisogno di sapere cosa dice al telefono.

I metadati sono così importanti che l'uomo che ha creato la Nsa per il Presidente Bush, il generale Michael Hayden – considerate che, almeno fino al 2014, Hayden riceveva la stessa intelligence che riceve ogni mattina il Presidente degli Stati Uniti, per darvi un'idea della potenza del personaggio - ha detto "noi uccidiamo le persone solo sulla base dei metadati". Hayden si riferiva ai droni americani che uccidono i presunti terroristi, usando proprio i proprio i metadati, che permettono di geolocalizzare il target da colpire: l'obiettivo viene individuato attraverso la posizione del suo telefonino, il drone opera una specie di finta cella telefonica a cui il telefonino del sospetto si aggancia per operare.

A quel punto, il drone ha individuato dove si trova il sospetto e può così ucciderlo, facendo partire un missile di cui il drone è fornito.

I metadati, che qui in Italia continuiamo a chiamare "tabulati telefonici" e che possono essere acquisiti dagli investigatori senza mandato, sono qualcosa di molto prezioso, altrimenti un'agenzia come la Nsa non avrebbe speso enormi risorse in termini di tempo ed energia per acquisirli.

Quando parliamo di Nsa, parliamo di un'agenzia che è grande tre volte la C.I.A. e che assorbe, da sola, un terzo delle risorse del budget degli Stati Uniti per l'intelligence che, vi fornisco un dato, nel 2015 è stato di 66,8 miliardi di dollari, nel 2014 di 67,9 e nel 2013 di 67,6 miliardi di dollari. Parliamo di un'entita di queste dimensioni.

Sentire il dottor Minniti dire che in Italia non c'è raccolta massiva di dati, quando questi documenti rivelano esattamente questo, cioè che dal 10 dicembre del 2012 al 9 gennaio 2013 l'Nsa ha fatto questa raccolta di metadati per oltre 45 milioni di telefonate, porta inevitabilmente a concludere che o i nostri servizi non dicono la verità o magari non sanno, oppure i documenti di Snowden sono falsi. Delle due l'una. Qualcuno si deve assumere la responsabilità di fare una dichiarazione del genere, vi assicuro che farà notizia in tutto il mondo se qualcuno si assumerà questa responsabilità di dire che non è vero, che i documenti di Snowden non sono veri.

C'è un forte contrasto tra quello che dicono le nostre istituzioni, i nostri servizi di intelligence e quello che dicono i documenti. Qualcuno non dice la verità. Chi non dice la verità?

Come ha dichiarato il procuratore Armando Spataro al nostro giornale in occasione della pubblicazione dei file di Snowden, "se sono veritiere le notizie e autentici i documenti pubblicati da L'Espresso - e non ho motivo di ritenere il contrario, vista la mancanza di smentite statunitensi", diceva il procuratore, "siamo di fronte ad un'attività chiaramente illegale. In Italia

eseguire intercettazioni o raccogliere dati informatici senza le dovute autorizzazioni giudiziarie è un reato".

Che io sappia, non c'è stata una procura che abbia aperto un'inchiesta per verificare quello che raccontano questi documenti. Si tratta di uno scandalo che è stato completamente lasciato scorrere via, come se non esistesse.

I documenti nell'archivio di Snowden sono ancora tanti, decine di migliaia o forse milioni e non è detto che non emergano intercettazioni anche su figure apicali dello Stato italiano. Sono emerse già intercettazioni, e io le ho pubblicate sul mio giornale, su tre Presidenti della Francia, sul governo tedesco, sulla Merkel e il suo entourage, sul governo giapponese e non è detto che non ci siano anche sul governo italiano e su figure apicali delle istituzioni italiane. Non è detto, perché quei documenti dopo tre anni devono ancora essere pubblicati.

Il fatto che vengano intercettati presidenti e capi di governo, in fondo, è "spionaggio" nel senso più classico del termine.

E lo spionaggio è il secondo mestiere più antico del mondo.

Ci può stare che intercettino i presidenti, ci può stare che intercettino il governo, quello che è nuovo è che intercettino intere popolazioni. Qui siamo di fronte a un fatto nuovo, questo è il problema.

C'è una sorveglianza che va oltre anche a quella della Stasi. Non attribuisco alla Nsa gli stessi metodi e le stesse intenzioni della Stasi, ma la sorveglianza Nsa va oltre quella della Stasi, perché l'organizzazione di spionaggio della Germania dell'Est non aveva a disposizione i mezzi e le risorse della Nsa. E i costi della sorveglianza, a quel tempo, erano immensamente più grandi.

Oggi, sapete quanto costa immagazzinare tutte le telefonate interne degli Stati Uniti su un *cloud* per un intero anno?

Si stima che costi solo 27 milioni di dollari. E' per questo che ho detto che la fattibilità tecnica, unita alla fattibilità economica, ha permesso alla Nsa di superare tutte le barriere e di creare la sorveglianza di massa su scala globale.

Qual'è la conseguenza di questo dato di fatto, che - ripeto - non è frutto di una paranoia? Come titola felicemente Greenwald nel suo libro, *"No place to hide"*, non c'è un posto in cui nascondersi; non c'è più. La conseguenza è questa.

In uno dei suoi libri migliori, Ross Anderson, professore di Sicurezza informatica all'Università di Cambridge, racconta che durante la guerra fredda nella Germania dell'Est erano ridotti a incontrarsi nei campi nudisti, per essere sicuri che almeno non venissero intercettati dalla Stasi. Andare a un appuntamento nudi era l'unico modo di essere sicuri che l'interlocutore incontrato non avesse nascosto nei vestiti dei dispositivi per registrare la conversazione o filmare l'incontro per conto degli agenti della Stasi.

Oggi neppure questa soluzione sarebbe più sufficiente, perché la tecnologia ha superato anche questo ostacolo. Ci sono microfoni che possono ascoltare e carpire le conversazioni da chilometri.

Personalmente, sono convinta che dobbiamo ancora mettere a fuoco e capire l'impatto e le conseguenze della società della sorveglianza di massa.

Siamo all'inizio: un po' come quando è stata scoperta la radioattività, gli scienziati ci giocavano con quel fenomeno misterioso che era la radioattività, appena scoperta: prendevano questi minerali e li appoggiavano sulla pelle delle braccia, per vedere che si formavano delle misteriose ferite, che richiedevano mesi per rimarginarsi. Erano chiaramente degli incoscienti, non avevano coscienza del danno. Così la società della sorveglianza di massa: non abbiamo ancora coscienza delle sue implicazione e dei suoi danni.

Ci siamo entrati quattordici anni fa, dopo l'11 settembre, silenziosamente, senza dibattito. Ce l'hanno fatta anche piacere, con Facebook, con i social, che sembrano un gioco innocuo, e ora ci ritroviamo dentro la società della sorveglianza di massa mani e piedi, con effetti devastanti.

Porto un'esperienza personale, non per esibirla ma perché è una cosa che ho vissuto: quando sono andata a incontrare le fonti

per accedere ai file di Snowden, sono stata seguita pesantemente, in modo plateale, a scopo intimidatorio. Non avevo assolutamente parlato con le fonti al telefono, non avevo parlato per mail, non le avevo contattate elettronicamente, l'unico dato che permetteva di capire le mie intenzioni erano le prenotazioni del volo e dell'hotel fatte dal mio giornale per permettermi di andare a incontrare le mie fonti. Non c'era altro.

Mentre andavo all'appuntamento con le fonti, sono stata seguita in modo plateale, per intimidirmi. A me è andata bene, ho avuto questo problema una sola volta, alla giornalista a cui Snowden ha consegnato i file, Laura Poitras, è successo quaranta volte in sei anni: fermata, interrogata alla frontiera, sequestrato ogni materiale, perché il suo lavoro era oggetto ad una pesantissima sorveglianza, quaranta volte.

La professione giornalistica non è l'unica ad avere questi problemi, anche i procuratori devono poter parlare con fonti e testimoni in condizioni di sicurezza, gli avvocati, gli attivisti per i diritti umani: come si possono svolgere queste professioni se non c'è la certezza della protezione delle persone con cui interagiamo?

Io parlo per me, per quello che ho vissuto: dopo tutta questa esperienza, vivo in una situazione per cui seguo rigorosi metodi di sicurezza, spendo molti soldi per la sicurezza informatica, seguo procedure penose, che limitano l'operatività sul campo. E questo è un problema che non si pone solo per la professione giornalistica, ma per tutte le professioni delicate.

E non è un problema che si pone solo per le persone che fanno lavori delicati: si pone per tutti, perché la sorveglianza di massa colpisce tutti. Se l'uomo della strada non fosse rilevante, se i suoi dati e le sue informazioni non servissero a nulla, la Nsa non spenderebbe soldi ed energie per intercettare tutti, prenderebbe solo le conversazioni dell'avvocato, del medico, del professionista. E invece prendono tutti.

Come si evolverà la società della sorveglianza di massa? Io non vedo un futuro ottimistico e se non arriveremo a un

dibattito serio, a serie riforme politiche, rischiamo che questa società della sorveglianza di massa si consoliderà con effetti devastanti sulla nostra democrazia e su quello che resta delle nostre libertà reali.

Vi ringrazio.

Licia Califano

Vorrei concludere con una riflessione su un aspetto della sicurezza che non deve assolutamente essere considerato secondario, e che al contrario necessita di un'attenta ponderazione: parlo della sicurezza dei dati, dei sistemi e delle reti.

Oggi le grandi banche dati e le reti strategiche rappresentano degli snodi nevralgici per ogni Paese, sia per le delicate funzionalità cui sono preordinate, sia perché sono in grado di rivelare una moltitudine di informazioni su ciascuno di noi, in alcuni casi anche connesse alla nostra sfera più intima.

Si pensi alle tante anagrafi istituite o in corso di istituzione (Anagrafe nazionale della popolazione residente, Anagrafe tributaria, Anagrafe nazionale degli assistiti, Anagrafe degli studenti, ecc.). Si pensi al Fascicolo sanitario elettronico e ai crescenti dossier sanitari attivi presso le singole strutture ospedaliere. Ma esistono anche un'infinità di archivi privati parimenti delicati, come ad esempio i sistemi di informazione creditizia, o i numerosissimi registri di utenti formati da banche, imprese di assicurazioni, società commerciali, fornitori di servizi telefonici e internet, ecc.

È quindi ineludibile l'esigenza di irrobustire le misure di *cybersecurity*, poiché attacchi informatici a reti e sistemi – per di più, in tempi di terrorismo globalizzato e ipertecnologizzato – possono realmente minare le democrazie quanto e più di attentati di tipo "classico".

L'impressione è che, oggigiorno, l'attenzione da parte di

mass media, opinione pubblica e istituzioni decidenti sia quasi del tutto focalizzata sulla predisposizione di misure di prevenzione al terrorismo "fisico". All'indomani della strage del Bataclan si sono immediatamente levate voci che spingevano verso l'indebolimento dei meccanismi di cifratura, in modo da consentire forme più pervasive di controllo: ma non dobbiamo mai trascurare che l'indebolimento delle forme di sicurezza digitale per ragioni di sorveglianza minerebbe altresì la fiducia dei cittadini e avrebbe ricadute gravi sulla società dell'informazione e sul voluminoso movimento economico ad essa connesso.

Dovremmo infatti tenere a mente episodi come, ad esempio, il grave *data breach* subito dalla Sony nel 2011, quando alcuni pirati informatici si sono impossessati dei dati personali di circa 77 milioni di utenti dei servizi Playstation, Network e Qriocity (di cui 1,5 milioni italiani): i terroristi di oggi stanno infatti dimostrando delle elevatissime competenze nell'utilizzo delle infinite potenzialità offerte dalle tecnologie informatiche, per cui occorre saper fronteggiare e azzerare anche la loro capacità di penetrazione dei sistemi.

Il Garante per la protezione dei dati personali si è da sempre dedicato con grande attenzione al tema della sicurezza delle reti e dei sistemi, e, in ultima battuta, dei dati personali che in questi transitano e si conservano.

Auspico quindi che gli sforzi effettuati in questo senso da parte dell'Autorità possano trovare continuità nell'azione del Parlamento, del Governo e di tutte le istituzioni preposte: perché al giorno d'oggi è molto più facile mandare in tilt un Paese aggredendo una delle sue banche dati strategiche, e questo, ai terroristi, non lo possiamo consentire.

Grazie a tutti.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Redazione
Garante per la protezione dei dati personali

Piazza di Monte Citorio, 121
00186 Roma
tel. 06 69677.1
www.garanteprivacy.it
e-mail: garante@gpdp.it

A cura del
Servizio relazioni esterne e media

Stampa:
UGO QUINTILY S.p.A.

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI