Diritto, Economia e Tecnologie della Privacy

Anno VI, Numero 1, 2015

Istituto Italiano Privacy

Editoriale

Contributi

Rassegna giuridica

Provvedimenti del Garante

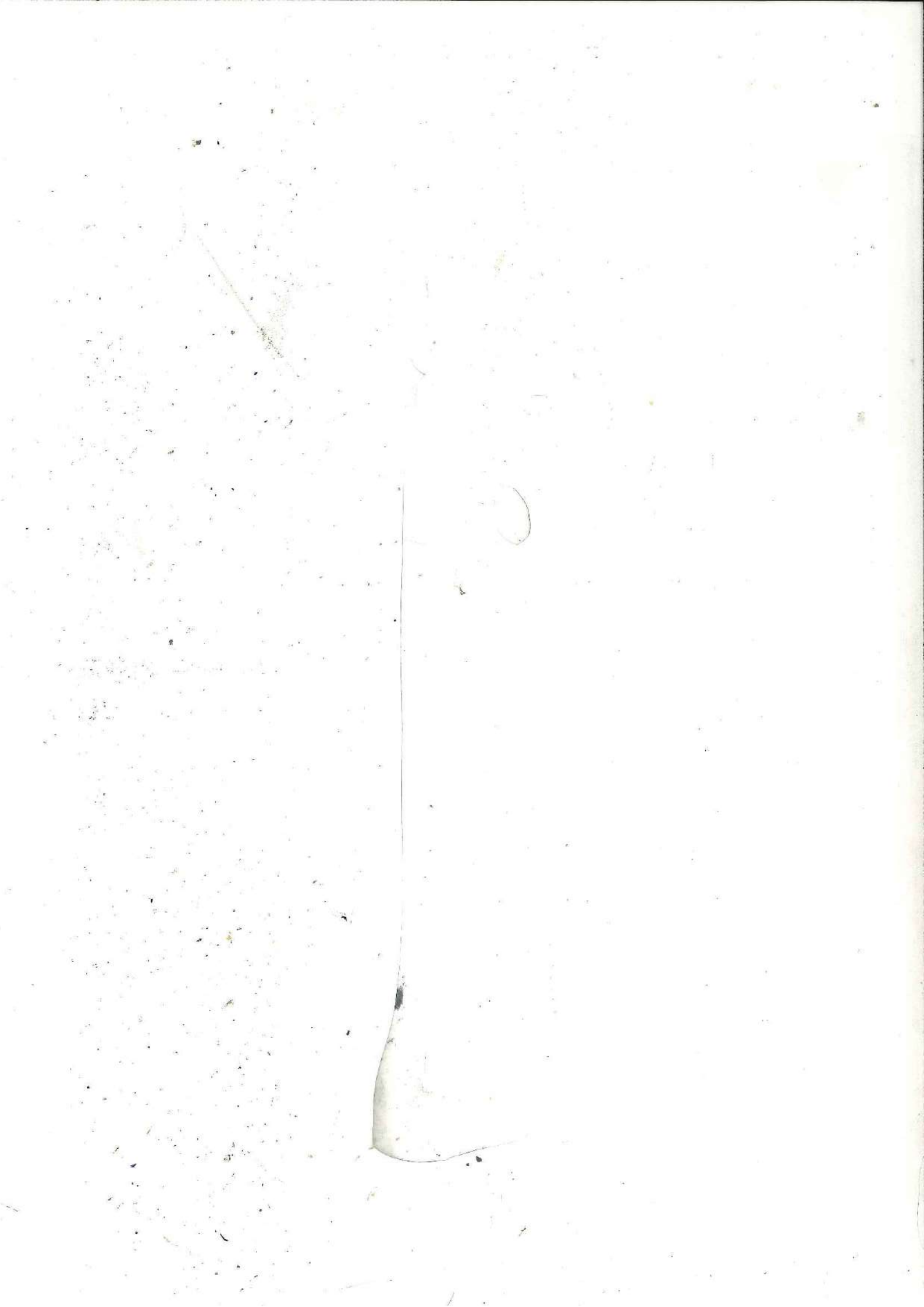
Giurisprudenza

ISTITUTO ITALIANO PRIVACY

ISSN 2239 -7671

Anno VI, numero 1, 2015 - Diritto, Economia e Tecnologie della Privacy

€ 25,00



Privacy versus security: considerazioni sul caso Snowden

di SERGIO FALCONE* e MARIO SCARAMELLA**

SOMMARIO: 1. Premessa. – 2. Privacy e Security: il sistema delle regole. – 3. Gli ambiti della privatezza. – 3.1. Il caso Snowden. – 4. Conclusioni.

1. Premessa.

Siamo abituati ad usare nel vocabolario giuridico italiano termini ed espressioni anglofone che abbiamo in molti casi importato dal sistema inglese o americano di *Common Law* senza tutto il loro relativo *background*. Non solo, alcuni istituti hanno senso solo laddove il caso giurisprudenziale sia ben noto, è il caso di espressioni come "*Osman Issue*" per indicare la "*preventability*" ovvero la responsabilità dello Stato o delle agenzie governative per non aver impedito qualcosa di prevedibile, oppure espressioni come "*Lawrence Case*" usata innanzi alle Corti del Regno Unito per criticare il modo in cui la polizia conduce indagini o ancora il termine "*Manson*" per riferirsi ai casi di morte a seguito di violenza razziale[1]: sono chiaramente questi dei casi giurisprudenziali vincolanti che nel sistema della *Common Law* sono divenuti, per la cogenza del giudicato e dei parametri, vera norma, legge. Non potremmo mai innanzi ad un Tribunale della Repubblica invocare "*Osman*" per intentare causa al Governo nel caso di morte di una personalità a cui fu negata la scorta, invece portiamo innanzi ai nostri tribunali

* Avvocato in Napoli e Presidente della Commissione Privacy e Security del Tribunale di Napoli.

** Consulente in materia di Privacy e sicurezza informatica.

[1] Questa rassegna di "istituti" è ad esempio riscontrabile nelle requisitorie dei Solicitors presso il Coroner di St. Pancras a Londra, che sta svolgendo una inchiesta con procedura "cornonial" prevista dal sistema inglese su i casi di morte violenta quali ad esempio l'omicidio Litvinienko e disponibili sul sito <www.litvinienkoinquest.org>.

violazioni di norme in materia di "Privacy" (o meglio di trattamento dei dati personali) ed in parlamento si dibatte di "Security" troppo invadente, senza che ai concetti importati da altri ordinamenti sia data la piena cornice sociale, politica e giuridica necessaria alla individuazione ontologica degli istituti o dei beni giuridici di cui dibattiamo.

Il concetto di sfera privata dell'individuo che dapprima le direttive della Unione europea e poi la legge dello Stato hanno introdotto nell'ordinamento, è ormai sufficientemente conosciuto e riconosciuto grazie al lavoro di implementazione della attenzione pubblica sul tema operato *in primis* dalla Autorità Garante e da varie organizzazioni (con o senza scopo di lucro), da siti web e riviste specializzate, analogamente a quanto hanno fatto in Europa gli alti paesi attenti alla "*public awareness implementation*" in materia di Privacy. Possiamo forse dire che essendo stato il concetto di Privacy (e la sensibilità verso questo bene giuridico oggi tutelato) "importati" in un primo momento proprio dal sistema anglosassone[2], la terminologia ancora adottata in Italia tradisce un'evoluzione sociale dove prima è arrivata la norma che individua e qualifica il bene e lo fa assurgere a valore, e solo poi la comunità apprezza il bene stesso e comincia a riconoscerlo. Forse nel nostro paese di "privacy" ne ha parlato prima il legislatore (attuando le direttive già vincolanti) e poi l'uomo comune, che solo oggi pretende la tutela della propria sfera privata ma che fino alla entrata in vigore della legge 675/96 e poi del D.Lgs. n. 196 del 30 giugno 2003, forse non immaginava neanche avesse piena valenza giuridica il proprio diritto alla sfera privata, alla riservatezza delle informazioni e dei dati personali al di fuori delle conosciutissime ma specifiche fattispecie previste dalla costituzione repubblicana e dal più antico codice penale, relative ad inviolabilità della corrispondenza, *domicilio et cetera*.

Laddove, generalmente, il diritto arriva a vestire situazioni preesistenti e realtà sociali, in questo caso è stato forse il diritto a creare una "domanda" di tutela dei dati personali e della sfera privata considerata nel suo complesso. Il vantaggio sociale è che questo vero

[2] Al 1890 risale il primo testo che inquadra l'istituto, S.D. WARREN E L.D. BRANDEIS, *The Right to Privacy*, 1890.

e proprio bene giuridico, forse qualificabile solo come interesse diffuso o quasi-bene fino a pochi anni orsono, è nato già disciplinato, la domanda si è strutturata intorno all'architettura voluta dal legislatore comunitario e poi nazionale che, per quanto complessa e articolata fra norme penali, civilistiche ed amministrative, pur in assenza di un esplicito riconoscimento costituzionale (pure concesso a beni giuridici di nuovo riconoscimento come ad esempio il diritto all'ambiente, grazie a leggi costituzionali recenti) ha indubbiamente il merito di aver dato alla protezione della sfera privata e dei dati personali una centralità nel sistema e nell' equilibrio dei valori tutelati dall'ordinamento.

Ogni Pubblica Amministrazione ed ogni azienda medio-grande presto dovrà munirsi di un *Privacy Officer*[3], ogni contratto ormai include clausole sulla Privacy, quasi ogni comportamento sociale e azione avente valore giuridico è condizionata dalla regolamentazione in materia di Privacy, non solo nei rapporti fra privati (regolati dal diritto civile) o fra amministrazione pubblica e privati (regolati anche dal diritto amministrativo) o nella repressione giudiziaria delle violazioni a norme sulla privacy penalmente sanzionate (sfera del diritto penale), ma addirittura nei rapporti di diritto pubblico, anche internazionale. L'era del cyber spazio ha poi consacrato la tutela dei dati personali in rete a vera e propria *salus populi* e la normativa sulla privacy a *suprema lex*, confermando l'impostazione che questo nuovo bene va tutelato per la sua centralità e prevalenza rispetto ad altri beni ed interessi.

2. Privacy e Security: il sistema delle regole.

Ma torniamo alla storia della tutela della privacy nel sistema anglosassone ed, in particolare, nel sistema americano. Non è questione prevalentemente giuridica ma sociale; in quel caso si è

[3] Il regolamento UE sulla protezione dei dati personali, che prevede l'introduzione della figura del *privacy officer*, la cui approvazione era per il maggio del 2014, probabilmente slitterà per dissidi tra Germania e Regno Unito in ordine alle intercettazioni USA.

trattato di mettere un vestito giuridico a realtà sociali molto sentite per quanto complesse: ebbene il concetto di Privacy non è indipendente da quello di "Security", la prima ha senso solo nella dicotomia *Privacy Versus Security* che ne specifica i limiti e la cornice sociale e poi giuridica, ma, soprattutto, istituzionale. E torniamo alla filologia dei termini che abbiamo importato nel nostro sistema senza conoscerne a fondo il significato: Security è un temine che possiamo trovare nel nostro paese associato alla regolamentazione dell'uso di un ascensore, all'accesso ad uno stadio sportivo, all'evacuazione di un immobile, possiamo trovar stampato "security" sulla casacca di un vigilante in spiaggia, sulla porta di emergenza di un ospedale. Ebbene in tutti questi casi il termine in lingua inglese o americana da utilizzarsi sarebbe *safety* e non *security*, ad indicare una sicurezza di tipo regolamentare, il rispetto di norme sulla prudenza da adottare per prevenire incidenti. È chiaro che in molti di questi casi il contrasto fra tutela della Privacy e assicurazione della Safety sarebbe da valutare e contemperare con grande equilibrio ed attenzione. La tutela di dati personali può arrivare ad incidere sugli standards di sicurezza? Posso, per esempio, negare il consenso all'utilizzo di mie informazioni personali laddove ne verrebbe compromessa la generale salubrità di un ambiente o il regolare funzionamento di infrastrutture?

Privacy Vs. Safety è certamente un serio confronto fra beni giuridici e fra interessi a volte forse contrastanti, ma sicuramente di pari intensità sociale e giuridica, soprattutto nel sistema anglosassone dove la tutela della sfera privata è molto sentita da tutti i cittadini da tempo immemorabile e parimenti riconosciuta. Una simile dicotomia esiste con molteplici beni ed interessi giuridici, la Privacy può essere in contrasto con altri valori che noi definiremmo costituzionali, ma che negli ordinamenti del Regno Unito (che non ha una costituzione scritta) e degli Stati Uniti d'America (che hanno una costituzione pluricentenaria mai ammodernata) sono semplicemente valori che la società riconosce, sente e tutela. La Privacy, ad esempio, può scontrarsi con esigenze di giustizia penale ed in paesi in cui il "giusto processo" esiste già da secoli, laddove noi abbiamo introdotto il concetto solo da pochi anni. È evidente che le garanzie fondamentali a tutela dei cittadini siano rigorose. Il potere autonomo e le garanzie sull'indipendenza della magistratura anche inquirente che sola può

violare i diritti inalienabili degli individui ed intercettarli, perquisirli, aprirgli la corrispondenza et cetera, costituisce in un certo senso una misura a tutela della privacy dei cittadini, misura supportata da molteplici istituti in materia di prova e presunzione di innocenza che limitano certamente le violazioni arbitrarie alla sfera privata.

3. Gli ambiti della privatezza.

Ma se non è di *Privacy Versus Safety* che per secoli si è dibattuto oltreoceano, e neanche di *Privacy Vs. Justice*, cosa ha delimitato davvero in maniera netta la sfera della "privatezza", cosa fin dalla sua stessa definizione ha compresso e ristretto in ambiti limitati quello che ormai è forse tra i primi diritti umani e sicuramente la bandiera di libertà per gli individui in ogni parte del mondo democratico? La parola "Security" è traducibile correttamente in "Sicurezza dello Stato", concetto che riguarda più il diritto internazionale degli Stati e le Istituzioni di Diritto Pubblico che qualsiasi altra branca del diritto, e che pertanto nella gerarchia delle fonti, trattandosi di diritto costituzionale pubblico interno e di altre norme la cui "opinio iuris ac necessitatis" è riconosciuta da secoli da parte della intera comunità internazionale, ha una prevalenza ed una riconosciuta importanza assoluta. *Privacy Versus Security* è il contrasto che ha portato alla definizione di quali sono o almeno dovrebbero essere i limiti nella tutela della sfera privata rispetto agli interessi fondamentali della sicurezza e della sopravvivenza dello Stato. È noto il brocardo attribuito a Cicerone che sintetizzava in "*salus populi suprema lex esto*"[4] il concetto che la sicurezza dello Stato deve essere la cosa a cui deve tendere la legge, a scapito dell'interesse degli individui, principio ripreso in tutte le moderne legislazioni e carte fondamentali che ovviamente (almeno in teoria) disciplinano le ingerenze dello Stato sui cittadini ed evitano le vessazioni, ma pur sempre riconoscono l'interesse superiore della esistenza e sicurezza dello Stato. Vi è spazio per una sfera privata del cittadino solo nell'ambito di uno Stato blindato nella propria sicurezza e pertanto capace di concedere quella

[4] CICERONE, *De legibus*, IV.

libertà individuale: questo è un istituto fondamentale rilevabile a livello comparato in ogni sistema. Ovviamente i paesi democratici regolamentano e soprattutto applicano strumenti a tutela della sfera privata che regimi dittatoriali negano o riconoscono fittiziamente a soli fini di propaganda. La più grande democrazia del mondo si è trovata comunque impreparata a discutere le questioni di Privacy Vs. Security: all'indomani dei primi attentati comunisti su suolo americano e con l'istituzione del *Federal Bureau of Investigation* diretto da Hoover a Washington, furono molteplici le forzature della legge esistente finalizzate a schedare e poi espellere cospiratori, fra il 1954 ed il 1971 [5] furono schedati tutti i membri di organizzazioni e movimenti sovversivi contro cui vi furono vere e proprie manipolazioni delle informazioni (ad esempio operazione Cointel Pro[6] e molti personaggi impegnati, ad esempio, in propaganda pacifista o antinuclearista o antirazziale furono oggetto di abusi). La reazione dell'opinione pubblica fu durissima tanto che il Congresso, ad esempio, istituì due comitati investigativi sull'operato dell'FBI. Tutto il "maccartismo", la pressione che l'anticomunismo istituzionale facente capo alla Commissione del Senatore McCarthy[7] produsse in termini di violazione della sfera privata di cittadini discriminati solo per le proprie (ipotizzate) idee politiche filo comuniste, divenne occasione del più ampio e approfondito dibattito di etica dello Stato che un paese moderno abbia affrontato.

Oggi a livello federale la normativa USA che disiplina le intercettazioni e le misure tecniche ha in sè i frutti garantisti del processo di discussione che ininterrottamente dal 1950 ad oggi, ha sviluppato la sensibilità sul tema, la disciplina è raccolta negli articoli

[5] JEFFREY – JONES, *FBI*, pag. 160; Warner Mac Donald 2005, Ransom 2007,

[6] La commissione del Congresso Usa accertò che l' FBI aveva compito di depistare, discrediare o distruggere informazioni su membri di movimenti antirazziali per la tutela dei neri e antimilitaristi contrari alle posizioni in Vietnam. COINTEL-PRO era una operazione pluriennale della FBI di Washington

[7] Tydings Cmtee, articolazione del Foreign Relations Cmte del Senato istituito nel febbraio 1950 per intraprendere «...uno studio completo ed esaustivo su quali siano gli individui traditori degli Stati Uniti che abbiano avuto o hanno un ruolo all'interno del Dipartimento di Stato»., il Presidente del sottocomitato era il Senatore Democratico Tydings mentre l' isipratore ed organizzatre della attività era il giudice e Senatore repubblicano McCarthy.

2510 e seguenti del Title 18, Parte I, Capitolo 119, dello US Code. Dopo la più grande, la più antica democrazia (la Francia) ha dovuto affrontare tardivamente il problema della Privacy regolamentando nel 1991 (legge n. 91-646 del 10/7/91) le intercettazioni dei servizi speciali e poi solo nel 2007, approvando una legge generale sulla materia del controllo dello Stato sulle situazioni istituzionalmente libere dei cittadini. In Germania, la normativa è quella degli articoli 100a e 100b del Codice di procedura penale e del regolamento 3/11/05 poi modificato dal Decreto di attuazione della Direttiva 2006/24/CE del 21 dicembre 2007. Il problema dell'eccessivo garantismo nei confronti degli ascolti dei servizi speciali è probabilmente figlio della serenità nelle relazioni internazionali successive alla caduta del muro di Berlino ed alla fine della Guerra Fredda.

Fino al 1991 i popoli delle grandi democrazie occidentali tolleravano che, per superiori interessi, i loro governi spiassero e quindi prevenissero infiltrazioni da parte di agenti comunisti pronti alla distruzione della civiltà in nome della ideologia. Francesi, inglesi, americani e tedeschi dell'*ovest* così come italiani, spagnoli, greci, nonostante le rispettive esperienze (alcuni paesi uscivano da dittature feroci come il regime dei colonnelli greci o il franchismo spagnolo) hanno tollerato in chiave anticomunista notevoli limitazioni della privacy, potremmo dire "per forza maggiore"; d'altronde l'esempio proveniente dai paesi oltrecortina riportava a scenari di azzeramento delle libertà personali e pertanto motivava ad una certa tolleranza verso i propri – pur opprimenti – apparati di sicurezza ed interessi nazionali, con il collasso dei regimi comunisti, lo scioglimento dell' URSS e del patto di Varsavia sia i paesi occidentali che le nuove democrazie si sono ubriacate di nuove e meravigliose libertà individuali e la ragion di Stato ha dovuto cedere il passo un po' ovunque ad una rafforzata tutela della sfera privata, anche con riferimento alla tutela dei dati sensibili, esaltata poi nel mondo senza frontiere che a livello regionale (Unione Europea con Shenghen) e globale (liberi mercati, WTO, internet e rafforzamento delle infrastrutture dei trasporti) dalla caduta delle barriere politiche ed economiche. Certo, il concetto di *Privacy Vs. Security* è rimasto tale in quei paesi dove entrambi i termini sono stati coniati, uno a delimitare

l'intensità dell'altro, sicuramente il primo subordinato al secondo. Nel nostro Paese e nella Europa continentale è arrivata forse l'idea di Privacy avulsa dalla sua cornice; ci è stato insegnato un diritto alla Privacy di intensità fortissima[8] e secondo a nessun altro principio, ci è stata raccontata una storia senza le sue premesse.

La minaccia alla Privacy dei cittadini è oggi un argomento di grande attualità sollevato da quello che, benché recentissimo, potremmo già definire il "caso Snowden" che ha portata globale. Un tecnico analista a contratto della National Security Agency (NSA) del governo degli Stati Uniti[9] è fuggito dapprima in territorio cinese e poi in Russia, portando con se copia di milioni di intercettazioni operate dalla sua Agenzia e quindi la prova di spionaggio illegale a carico di cittadini americani e stranieri, inclusi prominenti politici e capi di stati e di governi esteri. Snowden ha svelato al mondo che il governo degli USA spia un pò tutti ovunque. Proteste, non solo formali, sono state sollevate dalle cancellerie europee, *in primis* Francia e Germania, scuse e poco convincenti rassicurazioni sono state formulate dalla Casa Bianca ed un profondo dibattito, ancora una volta incentrato sulla etica di Stato e le incongruenze fra operato del governo e legislazione vigente, è iniziato in Europa e negli Stati Uniti.

Così posta, la questione sembrerebbe mettere in difficoltà un Presidente degli Stati Uniti, programmaticamente impegnato nella tutela dei diritti e delle libertà individuali e nel rasserenamento dei rapporti internazionali, per essere uno "spione" che tutto monitora e che da Fort Meade (sede della NSA) viola ogni intimità, tramite cellulari, telecamere, satelliti, carte di credito ed ogni altro strumento

[8] Oggi la privacy può essere definita come "il diritto di mantenere il controllo sulle proprie informazioni"- S. RODOTÀ, *Intervista tra privacy e libertà*, 2005.

[9] Edward J. Snowden informatico americano e consulente della Booz Allen Hamilton azienda a sua volta consulente della NSA, con la collaborazione di Glenn Greenwald, giornalista del Guardian, ha pubblicato una serie di informazioni su programmi di intelligence tra cui il protocollo di intercettazione telefonica USA ai danni di vari paesi fra cui membri della UE e della NATO (programmi PRISM, TEMPORA e altri programmi di controllo). Il 14 giugno 2013, l'Attorney General degli Stati Uniti ha formulato conro Snowden una denuncia, resa pubblica il 21 giugno, con accuse di furto di proprietà del governo, comunicazione non autorizzata di informazioni della difesa nazionale e comunicazione volontaria di informazioni segrete con una persona non autorizzata.

di comunicazione o controllo. La questione dal punto di vista giuridico si potrebbe ridurre a due fondamentali violazioni, la prima di diritto interno, a danno della Privacy dei cittadini americani, la seconda di diritto pubblico internazionale, per lo spionaggio illegale a danno dei paesi amici oltre che di quelli dichiaratamente nemici, ma richiede alcuni approfondimenti di carattere generale e storico. Per citare lo scomparso Presidente emerito della Repubblica Francesco Cossiga, che è stato anche Presidente del Consiglio e Ministro dell'Interno oltre che Ufficiale di Marina e gran studioso di questioni afferenti alla sicurezza nazionale, la sovranità stessa di un paese si esercita attraverso i suoi servizi segreti, mancando i quali un paese, appunto, non sarebbe sovrano[10]. Nel diritto internazionale è evidente, infatti, che non esiste una sicurezza comune a tutti, esiste solo una sicurezza dei singoli membri della comunità in competizione e contrasto fra di loro, un vero e proprio confronto fra Stati sovrani, una sicurezza internazionale sarebbe un ossimoro, una contraddizione in termini, laddove deve esistere una vigilanza, tramite gli apparati che raccolgono ed analizzano le informazioni, sulle minacce alla sicurezza dello Stato.

Le due sfide che si presentano allo Stato sovrano sono, dunque, quella interna, attacco da parte di individuo o organizzazioni presenti sul proprio territorio ed esterna, minaccia da parte di Stati o organizzazioni estere. Ogni paese ha, dunque, un proprio servizio di sicurezza interna e di sicurezza esterna che segretamente vigila su queste minacce. Si tratta di strutture diverse dalla polizia giudiziaria, che invece deve assicurare le prove per reati e che sono stati commessi ed arrestare i colpevoli ed anche di strutture diverse dalle forze armate che devono respingere attacchi militari. Si tratta di strutture di prevenzione che operano a livello segreto per assicurare allo Stato una perimetrazione politica di sicurezza sia interna che esterna. Bisogna ribadire due concetti, il primo è che ogni Stato per esistere ha bisogno di questi apparati, poiché ogni altro Sovrano ne dispone e pertanto l'equilibrio invisibile che definisce i confini geografici dell'uno e dell' altro si basa su quell'esercizio di sovranità che l'operatività dei servizi assicura (in altre parole se su di un territorio non se ne occupasse un

[10] S. DI GIOVANNI, *Intelligence da fonti aperte OSINT*, 2005.

servizio di sicurezza esso sarebbe occupato da un altro concorrente servizio a scapito della effettiva sovranità dello Stato titolare), inoltre bisogna sottolineare che si tratta di servizi generalmente definiti 'segreti' o 'speciali' perché essi, rispetto alle norme ed ai principi generali dei rispettivi ordinamenti operano in deroga. Il diritto costituzionale dei paesi occidentali non stabilisce, infatti, che il Governo possa spiare i cittadini, stabilisce però che elementi che possano produrre pregiudizio su cittadini, ad esempio, prove per un processo penale, siano acquisibili solo in alcune forme e sotto il controllo della Autorità Giudiziaria indipendente e che pertanto tutto quanto carpito con mezzi di spionaggio sia semplicemente inutilizzabile conto i diritti dell'individuo, *tamquam non esset.*

Il sistema più evoluto in tal senso è certamente quello britannico dove pur in assenza di Costituzione scritta il principio è esteso anche alle intercettazioni giudiziarie; la normativa in materia di ascolti è rappresentata dal *Regulation of Investigatory Powers Act* del 2000, integrato da codici di condotta (*Interception of Communication Code of Practice* 2002 e *Anti-Terrorism, Crime and Security Act* 2001) che escludono l'utilizzabilità in ambito giudiziario di qualsiasi intercettazione autorizzata, ovvero si spia ai fini di sicurezza nazionale ma quanto acquisito non è mai utilizzabile.

Conoscere elementi che potrebbero rappresentare una concreta minaccia all'esistenza stessa dello Stato, mantenendo segreti questi elementi, laddove, essi sono stati ottenuti in violazione di norme sulla privacy o laddove possano costituire una qualsiasi forma di ingerenza reale nella vita degli individui è lavoro legittimo delle agenzie per la sicurezza dello Stato. Questi elementi trattati in maniera sicura ed analizzati non potranno mai confluire in un file della polizia e costituire prova contro chicchessia perché ottenuti segretamente, in violazione di norme a tutela dei diritti fondamentali e comunque contrari a principi costituzionali e del giusto processo, ma potranno allertare il Capo del Governo ed i Ministri rispettivamente agli affari interno ed agli affari internazionali su questioni importanti e vitali. Non si tratta di riferire che Tizio o Caio hanno fatto questo o quello, ma si tratta di individuare profili della minaccia alla sicurezza e riferire a chi ha responsabilità di Governo che esiste questo o quel tipo di pericolo reale.

La responsabilità di un paese, come ad esempio gli USA, nei confronti dei propri cittadini e nei confronti della comunità internazionale si pone solo nel caso di abusi gravi e qualora ci si discostasse dalla prassi internazionale, si aumentasse eccessivamente l'intensità delle misure o si arrivasse a vere proprie operazioni clandestine illegali che invece di appartenere alla dimensione della intelligence dovessero realizzarsi in vere attività criminali. Ebbene, dobbiamo necessariamente valutare quale sia la situazione internazionale a livello di misure di *intelligence* dei vari paesi concorrenti con gli americani prima di valutare l'eventuale illiceità delle attività smascherate da Snowden. Bisogna poi ricostruire la defezione dell'analista NSA e le modalità con cui è stato sollevato lo scandalo e verificare effettivamente la portata dell' evento alla luce di possibili manipolazioni, per poi tentare una valutazione critica dell'accaduto.

3.1. Il caso Snowden.

Innanzitutto, dobbiamo ricordare che esiste un caso Snowden molto simile ed antitetico a quello che ha messo in imbarazzo gli USA ed è il caso Litvinienko, dal nome dell'ex tenente Colonnello del KGB poi divenuto Ufficiale dell'FSB, il servizio di sicureza interna della Federazione Russa. Ebbene Alexander Litvinienko si propose nel 2000 alla ambasciata americana in Turchia come defezionista e non fu da questi accettato (perché gli Usa non intendevano interferire con gli affari interni della Russia)[11], poi ottenne asilo politico dal Governo britannico senza che mai l'*intelligence* effettuasse un "*debriefing*", ovvero un completo interrogatorio su tutte le notizie conosciute dall'ufficiale (sempre perchè non si violassero accordi di rispetto reciproco fra super potenze) ed, infine, fu interrogato dalla "Commissione Parlamentare italiana sul *Dossier Mitrokhin* e sulla *Intelligence* istituita dalla Camera dei Deputati e dal Senato della Repubblica nella XIV Legislatura, alla quale passò oltre diecimila documenti relativi allo spionaggio russo operato ovunque e contro chiunque con mezzi elettronici avanzati.

[11] A. GODLDFARB, 2007.

Poche conseguenze sono derivate per le rivelazioni di Litvinienko, il quale riferì specificamente di un servizio, il FAPSI, omologo della NSA, capace di intercettare qualsiasi comunicazione sia sul territorio della Federazione Russa che all'estero. Non solo questo, il Colonnello Litvinienko riuscì a dimostrare, fornendo riscontri alle sue dichiarazioni registrate (oggi depositate all'antiterrorismo della Polizia Metropolitana di Londra), che l'*intelligence* russa utilizza giornali e televisioni nel mondo per diffondere le informazioni che più le aggradano, tramite una propria articolazione denominata "ZOST "e citando il caso del giornale inglese Guardian in un interrogatorio registrato in data 13 gennaio 2004. Se ne deve dedurre: 1) i russi fanno la stessa identica cosa degli americani; 2) che lo scandalo "Snowden" potrebbe essere stato montato ad arte nella escalation del confronto fra le potenze mondiali nuovamente contrapposte nello scacchiere tramite le strutture di propaganda.

Nessun dubbio che la NSA, gigante della amministrazione USA, che conta forse novantamila operatori addetti allo spionaggio elettronico ed ha un *budget* praticamente illimitato, faccia delle intercettazioni preventive un uso massiccio. Nessun dubbio che questa sorveglianza non sia limitata al solo territorio americano ma, tramite il sistema di *intelligence* delle comunicazioni e dei segnali denominato "Echelon" cui partecipano i paesi anglofoni (Canada, Uk, Austalia, Nuova Zelanda), da decenni spii il mondo intero. Positivo certamente il dibattito in corso sui i limiti che all'utilizzo di questa agenzia (e delle altre tredici agenzie specializzate in sicurezza della Amministrazione americana, strutturate in *intelligence* dei segnali, *intelligence* elettronica, *intelligence* delle immagini, *intelligence* militare et cetera) il Congresso americano deve porre in una ottica di etica pubblica sempre troppo trascurata, positivo infine che il confronto su questi temi avvenga per via diplomatica anche con i paesi europei amici (ed alleati nell'ambito del Trattato dell'Atlantico del Nord che ha compiuto i 65 anni e che si dimostra ancora molto attuale). Non corrispondente al vero però sarebbe nascondere che ogni paese ha la propria intelligence elettronica e che ci si spia a vicenda.

In Europa la Germania e la Francia (che hanno puntato il dito contro l'Amministrazione Obama per le verità smascherate da Snowden) sono certamente l'eccellenza nello spionaggio e nel

controspionaggio e sono state a loro volta toccate da scandali internazionali, ad esempio, quando fu scoperto e riportato dai media americani che i servizi francesi microfonavano l'intera *business class* della *Air France* per carpire i segreti della economia e far meglio competere il loro paese su questioni di mercato di beni e servizi. Risulta la presenza di navi addette allo spionaggio elettronico che battono tanto bandiera a stelle e strisce (come la USS Mount Withney oggi nel Mar Nero per i giochi olimpici a Sochi e generalmente di stanza a Gaeta, nave ammiraglia della VI Flotta un tempo gloriosa e che oggi conta solo questa unità) quanto bandiera tedesca (come riportato dal Corriere della Sera).

Ebbene dichiarava Litvinienko alla Commissione italiana di inchiesta che anche i russi hanno navi che intercettano tutti, gestite dal GRU il servizio centale militare, ed anche satelliti dedicati a questo servizio vi sono uffici dedicati all'ascolto di quanto si dice via internet. Vi sono satelliti spia franco-italiani (come il Cosmo Sky Med) e cinesi, forse i veri master del nuovo cyberterrorismo. Tutti spiano tutti e l'individuo è certamente mortificato da questa realtà internazionale che però trova un suo equilibrio proprio nella pluralità di strumenti ed attenzioni. È evidente che non potrebbe oggi il solo governo di Washington interrompere gli ascolti lasciando la Russia sola a fare *intelligence* delle comunicazioni.

I Governi delle democrazie occidentali sono costretti a monitorare la sicurezza dei loro paesi con tutti gli strumenti che l'*intelligence* mette loro a disposizione[12] e nei limiti di utilizzo prescritti nelle carte fondamentali e nelle leggi, ciò significa che mai le informazioni raccolte a 360° potranno essere utilizzate contro singole persone violate nella loro privacy da strumenti invasivi, mai l'*intelligence* sarà prova giudiziaria contro individui, mai il lavoro dei servizi segreti incriminerà questo o quel cittadino. Mai le informazioni usciranno dal circuito chiuso dei carteggi segreti e classificati, i cui destinatari potranno essere al massimo il Ministro con delega ai servizi ed i servizi omologhi dei paesi alleati, mai l'Autorità Giudiziaria o la

[12] L'FBI ha considerato tra le priorità del 2013 quella di sorvegliare "Gmail e Skype", perchè nell'era digitale i terroristi comunicano con protocolli protetti, anche con i videogiochi.

Polizia potranno divenire recipienti di questi dati raccolti in violazione della Privacy dei cittadini. È quanto accade negli USA ad esempio con la banca dati sull'antiterrorismo denominata "T.I.D.E.", gestita da apposita agenzia che ha schedato almeno 850.000 persone, cui possono accedere solo le agenzie di *intelligence* e che solo in versione molto degradata, senza nomi e fatti specifici, è accessibile anche alla FBI. Il limite posto dagli ordinamenti nei paesi democratici è, infatti, quello della non utilizzabilità della gran quantità di dati di *intelligence*, raccolti perché fenomeni siano conosciuti da chi ha la responsabilità di prevenire attacchi alla sicurezza dello Stato, ma che non possono essere comunicati alla A.G. o ad altre autorità (ad esempio il Parlamento) ed ovviamente alla opinione pubblica.

Ancora una volta il Caso Litvinienko ci offre un esempio molto rilevante al proposito. Essendo stato il colonnello del KGB\FSB ucciso su territorio britannico nel novembre 2006 con una sostanza radioattiva, la polizia giudiziaria (Antiterrorismo della Polizia Metropolitana di Londra denominato SO15) ha avviato un'indagine criminale e la Procura della Corona ha incriminato due ex agenti segreti russi, oggi ricercati in campo internazionale. Il processo non si è potuto celebrare per la mancata estradizione dei sospetti da parte russa. Un giudice della Alta Corte in funzione di Coroner, ovvero di ufficiale indipendente incaricato di verificare le corcostanze di una morte violenta, ha poi avviato un'inchiesta (Inquest) ed ha chiesto accesso ai documenti ed alle informazioni in possesso del Governo il quale ha posto il PII (dichiarazione di immunità per interesse pubblico prevalente), ovvero, ha secretato tutto dichiarando che *prima facie* si evince la responsabilità dello Stato russo ma che non possono essere divulgate le informazioni di *intelligence* ad autorità terze; il Governo ha anche negato l'apertura di una "*Inquiry*" che a differenza della "*Inquest*" potrebbe accedere a documenti classificati[13]. L'inchiesta dovrà essere fatta solo sulla base di informazioni non provenienti dalla comunità di *intelligence*. Abbiamo la prova, quindi, di come tutto il materiale prodotto da MI6 (intelligence estera) MI5 (intelligence interna) e GCHQ (intelligence delle comunicazioni governative) non

[13] Tutto quanto conerne l'inchiesta Litvinienko ed i riferimenti procedurali è consultabile sul sito ufficiale dello Stato britannico www.litvinienkoinquest.org.

possa mai confluire in circuiti diversi dalla *intelligence* (es. processo penale o inchiesta del Coroner) nemmeno nel caso iperbolico dell' assassinio di una spia a Londra con il mezzo del terrorismo nucleare (il Colonnello fu avvelenato con il polonio radioattivo che contaminò anche altre decine di persone). Inoltre, le informazioni passate da Litvinienko alla Commissione Parlamentare di Inchiesta sulla *Intelligence* sono state girate in almeno due occasioni dalla Commissione alla polizia giudiziaria (stante la gravità dei fatti riferiti) ed in entrambi i casi la A.G. ha ritenuto illegale la trasmissione di dati di *intelligence* alla Polizia Giudiziaria[14].

4. Conclusioni.

Da questo spaccato possiamo evincere che la massiccia attività di spionaggio elettronico operata dai servizi di sicurezza per quanto vessatoria nei confronti dei diritti dei cittadini e violativa della Privacy sia generalmente contenuta nei limiti dei principi generali dell' ordinamento e che il danno effettivo alla sfera degli interessi privati sia in realtà minimo. Si consideri che in Italia le stesse intercettazioni preventive dei servizi segreti devono essere autorizzate dalla A.G. (Procura Generale della Repubblica presso la Corte di Appello di Roma ex L. 133/2012), la quale pertanto vigila su abusi e vaglia le richieste perché le esigenze di Security non arrivino automaticamente ad annullare il diritto alla Privacy. In quest'ambito, di recente è stato siglato un protocollo di intesa tra il Garante per la protezione dei dati personali ed il DIS (Dipartimento delle informazioni sulla sicurezza)[15] con l'obiettivo di aumentare i controlli sulle attività di *intelligence* già previsti dalla legge. L'accordo si propone di dare risposta all'esigenza di sistematizzare i controlli del Garante, già previsti dalla normativa vigente, che si affiancano a quelli del Copasir (Comitato parlamentare per la sicurezza della Repubblica) e dell'Autorità giudiziaria (questi

[14] Sentenza 361\08 GIP 25° Tribunale di Roma del 14.02.08 e Sentenza n. 2602\12 Tribunale di Rimini del 30\11\2012.

[15] Il protocollo d'intesa è stato siglato in data 11.11.2013 presso la Presidenza del Consiglio dei Ministri.

ultimi relativamente ai dati sulle comunicazioni), completando la somma di garanzie a presidio del trattamento dei dati personali da parte delle Agenzie di informazione. In particolare nel protocollo vengono richiamate le modalità di esecuzione degli accertamenti del Garante nei confronti delle Agenzie di Informazione e prevede la comunicazione al Garante del piano ricognitivo degli archivi informatici cui il DIS e le Agenzie hanno accesso ai sensi dell'art. 13, comma 2 della legge 124 del 2007, e le acquisizioni di dati effettuate in attuazione dell'art. 11 della direttiva sulla sicurezza cibernetica[16].

Caso diverso è quello delle intercettazioni ad uso giudiziario dove il notevole ricorso alle misure tecniche[17], in un sistema dove in realtà non è l'*habeas corpus* ma il "libero convincimento" del giudice a motivare misure limitative della libertà personale come l'arresto, costituisce una minaccia alle libertà fondamentali degli individui[18], ma questa non è questione di Privacy Vs. Security, è un problema di politica criminale e di amministrazione della giustizia[19] che nulla ha a che vedere con le (in realtà più innocue perchè inutilizzabili) intercettazioni preventive dei servizi segreti.

Che il caso Snowden-Guardian rappresenti l'efferatezza della guerra tra agenzie di *intelligence* e non la prova di responsabilità dei governi lo dimostra l'epilogo della vicenda: con duecentocinquanta milioni di budget i giornalisti autori dello scoop del caso Snowden hanno istituito una piattaforma di propaganda denominata *The*

[16] D.M. 24 gennaio 2013 pubblicato in Gazz. Uff. 19 marzo 2013 n. 66.

[17] Le intercettazioni sono consentite, previa autorizzazione al P.M. concessa con decreto motivato dal G.I.P., in relazione a delimitate gravi ipotesi delittuose (analiticamente indicate dall'art. 266 c.p.p.) e solo *"quando vi sono gravi indizi di reato e l'intercettazione è assolutamente indispensabile ai fini della prosecuzione delle indagini"* (art. 267 c.p.p.).

[18] Lo stratagemma, non di rado utilizzato, per di poter disporre le intercettazioni, è la contestazione del reato di associazione a delinquere, ipotesi criminale idonea a consentire indagini su reati meno gravi, ma che tante volte non è stata più ravvisata al termine delle indagini stesse.

[19] Un tentativo di mettere ordine nella materia delle intercettazioni e quindi di bilanciarle con la disciplina del trattamento dei dati personali è stato effettuato con il disegno di legge n. 1611/2006, che però è ancora fermo per l'approvazione alla Camera dei Deputati. Il d.d.l. prevede, tra l'altro, il divieto di pubblicazione delle intercettazioni fino al termine delle indagini preliminari.

Intercept, consultabile direttamente in internet dagli utenti ed interamente criptata a livello governativo (un vero gioiello di crittografia spionistica) sulla quale si propongono di raccogliere qualsiasi informazione segreta, tipo quelle di Snowden per l'appunto, nel pieno anonimato dei confidenti-defezionisti al fine di dimostrare asserite pratiche irregolari delle amministrazioni centrali. Un vero "*breaktrought*", salto in una nuova dimensione della minaccia alla sicurezza degli stati, dove qualunque ufficiale o funzionario può ammutinarsi e mettere in seria difficoltà il proprio paese, in tutta sicurezza, con un *click* sulla sua tastiera.