Gli USA e la sorveglianza sugli stranieri nel post-9/11: riflessioni a margine del rinnovo della sez. 702 FISA

di Chiara Graziani

Title: The US and surveillance of foreigners after 9/11: some comments on the reauthorization of sec. 702 FISA

Keywords: USA; Surveillance; National security.

1. – Il 19 gennaio 2018, il Presidente degli Stati Uniti, Donald Trump, ha firmato il *FISA Amendments Reauthorization Act*. Per mezzo di questa legge, è stata rinnovata per ulteriori sei anni – dunque, fino al dicembre 2023 – l'applicazione della sez. 702 del *Foreign Intelligence Surveillance Act* (nel prosieguo, FISA). Il FISA, entrato in vigore nel 1978 per regolare le procedure volte ad attuare misure di sorveglianza nei confronti di soggetti non aventi cittadinanza statunitense, non conteneva, nella sua originaria versione, la sez. 702. L'introduzione di tale norma, particolarmente controversa per le ragioni che si andranno ad esaminare a breve, risale al 2008 e si deve ad una delle numerose revisioni del FISA che il legislatore statunitense ha ritenuto necessarie dopo gli avvenimenti dell'11 settembre 2001 (*FISA Amendments Act* 2008) e il conseguente picco della minaccia alla sicurezza nazionale.

Il presente lavoro commenta il recente rinnovo del FISA e trae spunto da esso per ulteriori riflessioni. L'analisi si articola come segue. In primo luogo, si ripercorrerà lo sviluppo normativo sulla sorveglianza, con specifica attenzione per le comunicazioni tra cittadini americani e soggetti stranieri, attuata dalle agenzie governative statunitensi. Successivamente, si ricostruirà la giurisprudenza sulla questione, analizzando l'evoluzione dell'atteggiamento delle corti statunitensi nel bilanciare il diritto alla *privacy* e alla protezione dei dati con gli interessi confliggenti (fra i quali, in particolare, la sicurezza nazionale). Ci si concentrerà poi sul *FISA Amendment Reauthorization Act*, approvato nel gennaio 2018, al fine di esaminarne nello specifico le disposizioni e di rilevare se si sia trattato di un puro e semplice rinnovo nel tempo, che lascia la disciplina normativa identica a quella del passato, oppure se vi siano alcune rilevanti differenze. Alla luce del quadro tracciato, nella sezione conclusiva si svilupperanno riflessioni critiche, dalle quali emergerà l'evoluzione – a livello globale – del concetto di sorveglianza. In parallelo, si delineerà l'influenza del regime statunitense in tema di *privacy*, che sta assumendo connotati sempre meno garantistici, sui rapporti con altri attori della scena internazionale, e, nello specifico, del versante europeo.

2. – Il FISA viene approvato nel 1978, successivamente ai noti scandali emersi durante la presidenza Nixon, e recepisce una serie di principi che, nel corso degli anni, sono emersi da varie decisioni della Corte Suprema, nonché dai dibattiti in seno al Congresso, in relazione all'applicazione del Quarto Emendamento alla sorveglianza elettronica (per

un'analitica ricognizione dei precedenti storici, sia legislativi sia giurisprudenziali, dei dibattiti in Congresso relativi al FISA, nonché dei principali aspetti da esso disciplinati, si rinvia ad A.R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act 1978*, in 137 *University of Pennsylvania Law Review* 793, 794 (1989); si veda anche L.K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, in 37 *Harvard Journal of Law and Public Policy* 757, 766 (2014)).

La versione originaria della normativa in esame prevedeva che, qualora il governo, tramite le proprie agenzie, intendesse porre sotto sorveglianza le comunicazioni tra i cittadini americani e quelli stranieri che avessero avuto luogo in territorio statunitense, dovesse preventivamente rivolgersi ad un apposito giudice, la c.d. *FISA Court* (un organo giudicante speciale istituito dallo stesso FISA), per l'ottenimento dell'autorizzazione (c.d. *warrant*). Al fine del rilascio del *warrant* da parte della corte specializzata, era necessario che il governo dimostrasse che il *target* delle misure di sorveglianza – ossia il cittadino straniero con cui il cittadino americano si relazionava – fosse qualificabile come «foreign power» oppure «agent of a foreign power». Pertanto, l'applicazione di tali tecniche di sorveglianza risultava soggetta al sindacato preventivo di una corte, benché si trattasse di un giudice *ad hoc*. A tale proposito, in effetti, appare opportuno rilevare come, a giudizio della dottrina americana che ha commentato la disciplina stabilita dal FISA nei primi anni successivi la sua entrata in vigore, la *FISA Court* – la quale, peraltro, opera ancora oggi con udienze segrete – si pone in violazione dell'art. 3 della Costituzione statunitense, relativo al potere Giudiziario, e del Quinto Emendamento, che consacra la c.d. *due process clause* (v. A.N. Kornblum, L.M. Jachnycky, *America's Secret Courts – Listening in on Espionage and Terrorism*, in 24 *Judge's Journal* 14, 15 (1985); per una disamina più recente del punto, S.I. Vladeck, *The FISA Court and Article III*, in 72 *Washington and Lee Law Review* 1161 (2015)). Si noti, tuttavia, che, nel quadro originario, questa forma di *judicial review* che operava *a priori* – pur discutibile nel suo funzionamento concreto, a causa della specialità del giudice e della segretezza delle udienze – era applicabile solo nel seguente caso: qualora la sorveglianza riguardasse comunicazioni tra cittadini statunitensi e cittadini stranieri localizzate *in territorio statunitense*. La stessa affermazione può essere fatta in relazione alla limitazione soggettiva (le misure di sorveglianza erano attuabili solo qualora lo straniero fosse qualificabile come «foreign power» oppure «agent of a foreign power»), anch'essa valida solo nel caso appena citato. Al contrario, qualora le comunicazioni tra cittadini non statunitensi e cittadini statunitensi avessero luogo *nel territorio di paesi terzi* – si entra, pertanto, nella fattispecie della comunicazione internazionale – non si faceva più riferimento al FISA, con le relative garanzie, ma all'*Executive Order* 12333/1981, firmato dal Presidente Reagan e avente lo scopo di stabilire linee guida relative all'attività di *intelligence* posta in essere dai servizi segreti statunitensi (per un'approfondita trattazione del suo contenuto prima della modifica del 2008, di cui si parlerà, si rinvia a S.J. Conrad, *Executive Order 12,333: Unleashing the CIA Violates the Leash Law*, in 70 *Cornell Law Review* 968 (1985)). Secondo tale fonte, non vi erano limiti alla raccolta e analisi dei dati derivanti da comunicazioni internazionali. Tuttavia, come recente dottrina non manca di rilevare (E. Goitein, *Another Bite out of Katz: Foreign Intelligence Surveillance and the Incidental Overhear Doctrine*, in 55 *American Criminal Law Review* 105, 108 (2017)), nonostante tale disciplina fosse particolarmente permissiva nei confronti delle interferenze statali e, parallelamente, poco garantista nei confronti dei soggetti intercettati, nel momento in cui essa è stata approvata vi era un'ingente quantità di limiti tecnologici. Questi ultimi rendevano, di fatto, la comunicazione internazionale – e, di conseguenza, la relativa sorveglianza – molto difficile da porre in essere sul piano concreto. Pertanto, si può sostenere che, almeno nei suoi primi anni di vigenza, tale normativa abbia scontato limiti tecnici, ancor prima che giuridici.

Diverso, invece, è il contesto odierno. In effetti, il quadro giuridico descritto cambia nel 2008. Come si è già detto, in tale anno il *FISA Amendments Act* entra in vigore – sostituendo, peraltro, la più garantistica legislazione del 2007, il *Protect America Act* – e dà

vita alla sez. 702 FISA. In base ad essa, il governo statunitense non necessita più dell'autorizzazione preventiva (c.d. *warrant*) da parte della *FISA Court* per porre in essere, grazie ai servizi di *intelligence*, misure di sorveglianza sulle comunicazioni che avvengono in territorio americano tra cittadini statunitensi e non. Inoltre, tale sorveglianza può essere applicata indiscriminatamente, senza cioè nessuna necessità di dimostrare che il cittadino straniero con cui il soggetto americano intrattiene le proprie comunicazioni sia qualificabile come «*foreign power*» o «*agent of a foreign power*». La sorveglianza, in tale contesto, può essere autorizzata *dall'Attorney General* o dal direttore della *National Intelligence*, al fine dell'acquisizione di «foreing intelligence information». Inoltre, la sorveglianza sugli stranieri in territorio estero non è più disciplinata dall'*Executive Order* 12333/1981, ma dallo stesso FISA (più ampiamente sulle modifiche intervenute nel 2008, v. L.K. Donohue, *Section 702 and the Collection of International Telephone and Internet Contents*, in 38 *Harvard Journal of Law and Public Policy* 117 (2015).

In parallelo, nello stesso anno, vengono apportati degli emendamenti ad altri aspetti dell'*Executive Order* 12333/1981 da parte dell'Amministrazione Bush. Il Presidente Bush adotta l'*Executive Order* 13470/2008, nell'intento di aumentare, in maniera esponenziale, i poteri del direttore della *National Intelligence*. Tali modifiche rispondono alla necessità di adeguare la disciplina contenuta nell'*Executive Order* in parola a quella che viene ritenuta la più rigida e omnicomprensiva legislazione antiterrorismo di tutti i tempi, ossia il *Patriot Act*, approvato nel 2001 in risposta agli attacchi dell'11 settembre. Invero, anche la revisione del FISA attuata nel 2008 appare rapportabile a tale esigenza (G. Resta, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in G. Resta, V. Zeno-Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai "Safe Harbour Principles" al "Privacy Shield"*, Roma, 2016, 23, 33). In effetti, entrambi gli emendamenti del 2008 vanno nella direzione di affidare poteri sempre più ampi a soggetti rispondenti all'esecutivo, nell'ottica fissata, in via generale, proprio dal *Patriot Act* del 2001.

In contemporanea a tali modifiche legislative, non si può prescindere dal tenere conto di un altro fattore, non riguardante il piano giuridico, bensì quello tecnico, ossia il forte sviluppo tecnologico che si è affermato nei primi anni del XXI secolo – quindi, esattamente a cavallo dell'*escalation* della minaccia posta dal terrorismo internazionale. Se prima le comunicazioni internazionali costituivano un'ipotesi remota, in quanto richiedenti alti costi e strumentazioni sofisticate, negli anni successivi al 2000 diventa sempre più semplice e relativamente economico relazionarsi con persone che si trovano in qualsiasi parte del mondo: si pensi solo alla diffusione delle e-mail o di Skype. Come è facile immaginare, lo sviluppo della tecnologia non opera solamente a favore dell'utente, quindi del sorvegliato, ma anche a beneficio dei sorveglianti: la strumentazione a disposizione dei servizi di *intelligence* per realizzare misure di raccolta e conservazione di dati diventa sempre più efficace e rapida.

Ritornando agli aspetti giuridici, occorre non dimenticare che, stante l'ampia diffusione delle comunicazioni internazionali che ha caratterizzato l'ultimo decennio, il quadro normativo sopra descritto è afferente al caso in cui lo scambio di informazioni avvenga tra cittadino americano e quello non americano (in territorio statunitense o, dopo la modifica del 2008, anche in territorio estero). Qualora, invece, sia necessario porre sotto sorveglianza le comunicazioni tra cittadini americani, anche su territorio estero, risulta applicabile una differente disciplina, costituita dalla sez. 215 del *Patriot Act*, originariamente soggetta a *sunset clause*, ma più volte rinnovata, fino all'approvazione, nel 2015, dello *US Freedom Act*. Quest'ultimo la riproduce in termini quasi identici (per una breve analisi della legge da ultimo citata, F. Boehm, *Assessing the New Instruments in EU-US Data Protection Law for Law Enforcement and Surveillance Purposes*, in 2 *European Data Protection Law Review* 178, 183 (2016)). La sez. 215 del *Patriot Act*, da un lato, applica le regole proprie della sez. 702 del FISA anche alla sorveglianza sui cittadini americani all'estero, essendo pertanto il regime giuridico sostanziale uguale a quello applicabile ai cittadini stranieri; dall'altro, però, pone alcune differenze a livello processuale, poiché prevede che, per quanto riguarda i cittadini statunitensi, i risultati delle intercettazioni

siano utilizzabili come prove in sede giurisdizionale solo qualora sia in corso un'indagine avente ad oggetto atti di terrorismo internazionale o di spionaggio. Si affermano, quindi, rilevanti limitazioni al concreto utilizzo di tali informazioni. Benché il presente contributo si soffermi sulla sorveglianza di comunicazioni tra cittadini americani e cittadini stranieri entro i confini degli Stati Uniti o al di fuori di essi, tale precisazione risulta necessaria ai fini di una più completa delineazione del quadro normativo di riferimento.

La sorveglianza sugli stranieri da parte dei servizi di *intelligence* statunitensi appare, perciò, particolarmente invasiva. Il regime imposto dalla sez. 702 del FISA sarebbe dovuto venire a scadenza nel gennaio 2018, ma, come si è visto, il Congresso ha prontamente approvato il *FISA Amendments Reauthorization Act*, che rinnova l'applicabilità del FISA come modificato nel 2008. Prima di prendere in esame in maniera più approfondita l'atto legislativo del 2018 e sul contesto in cui esso è entrato in vigore, occorre ricostruire, seppure sinteticamente, talune problematiche sollevate dalla sez. 702 del FISA e, soprattutto, la loro soluzione sul versante giurisprudenziale.

3. – In primo luogo, è opportuno ricordare che la tutela del diritto alla *privacy* viene desunta dal Quarto Emendamento della Costituzione statunitense, il quale offre protezione contro «unreasonable searches and seizures»; condizione che legittima il governo a tali intrusioni è, secondo la Costituzione, l'ottenimento di un «warrant», che ne certifichi la ragionevolezza.

Occorre, dunque, richiamare la teoria tradizionale che le corti americane adottano per bilanciare il diritto individuale alla *privacy* e interessi con esso confliggenti. A tal proposito, al fine di verificare se debba essere la *privacy* o l'interesse opposto a prevalere, la Corte Suprema, nella decisione *Katz* (*Katz v. United States*, 389 U.S. 347 (1967)), ha fissato il c.d. *reasonable expectation test*. In base ad esso, il diritto alla *privacy* prevale solo qualora l'individuo possa avere una "ragionevole aspettativa" di tutela della propria vita privata. In caso contrario, l'interferenza nella vita privata è legittima – sempre a condizione dell'esistenza di un valido *warrant*. Portato dello *standard* della *reasonable expectation* è la c.d. *third-party doctrine*, sviluppata dalla Corte Suprema nelle sentenze *United States v. Miller* (425 U.S. 435 (1976)) e *Smith v. Maryland* (442 U.S. 735 (1979)). In base ad essa, un individuo non può rivendicare la ragionevole aspettativa di tutela del proprio diritto alla *privacy* qualora egli abbia volontariamente messo a disposizione di un terzo (es. una banca o un operatore telefonico, ma anche, nell'era della tecnologia, un *service provider*) i propri dati personali. Si tratta, chiaramente, di un orientamento molto restrittivo, giacché la sua applicazione legittima molteplici limitazioni del diritto alla *privacy*, peraltro facilmente giustificabili. La recente dottrina americana tende a ritenere la *third-party doctrine* obsoleta nell'era digitale, in cui, da una parte, il trasferimento dei metadati rappresenta la *conditio sine qua non* per l'accesso a taluni servizi e, d'altra parte, non si può ragionevolmente affermare che il consenso al loro trattamento ad opera di un particolare destinatario – nello specifico, il *service provider* – possa essere considerato alla stregua del consenso a metterli a disposizione di un pubblico generalizzato e, in particolare, delle agenzie governative (in questo senso, M.W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, in 8 *Journal of National Security Law and Policy* 247, 276 (2015)).

L'organo giurisdizionale che ha modo di esprimersi sulla sez. 702 FISA è rappresentato, in un primo momento, dalla sola *FISA Court*. Infatti, benché, dopo il 2008, venga abrogata la sua competenza di attuare un vaglio preventivo, nell'autorizzare le misure di sorveglianza, essa conserva la competenza a controllare, almeno *a posteriori*, la legittimità di quanto posto in essere *ex* sez. 702. Dopo il 2013, invece, anche le corti ordinarie hanno l'opportunità di occuparsi della questione, poiché il governo statunitense, al contrario di quanto accadeva negli anni precedenti, inaugura la prassi di notificare ai soggetti sottoposti a sorveglianza l'utilizzo processuale delle informazioni ottenute. Di conseguenza, tali individui si trovano nella possibilità di contestare la legittimità delle

misure delle quali sono stati oggetto e, pertanto, l'utilizzabilità dei relativi dati come prove nel corso di un processo a loro carico.

I giudizi relativi all'impiego della sez. 702 FISA si incentrano, principalmente, su due questioni giuridiche: in primo luogo, se sia o meno legittimo porre in essere tale sorveglianza senza necessità, da parte del governo, di ottenere alcuna autorizzazione (*warrantless surveillance*); in secondo luogo, come vada affrontata la tematica del c.d. *incidental overhear*. A proposito di quest'ultimo punto, il problema si pone nei seguenti termini: nel porre sotto sorveglianza il *target* straniero, i servizi di *intelligence* possono "accidentalmente" intercettare le informazioni relative all'interlocutore, che è cittadino americano. Si tratta, dunque, di intercettazioni di coloro che non rientrano fra i *targets* mirati delle misure in esame.

La posizione della giurisprudenza statunitense su entrambi i temi menzionati è desumibile da tre decisioni, tutte emesse da corti distrettuali, non essendosi la Corte Suprema ancora pronunciata sul punto: *United States v. Muhtorov* (187 F. Supp. 3d 1240 (D. Colo. 2015)); *United States v. Mohamud* (843 F.3d 420 (9th Cir. 2016)); *United States v. Hasbajrami* (1:11-cr-00623 (E.D.N.Y. 2016), tutte riguardanti l'applicazione della sez. 702 FISA. Tali sentenze, prevedibilmente, fanno leva anche su principi elaborati, negli anni precedenti, dalla *FISA Court*. Senza soffermarsi specificamente su ciascuno dei casi richiamati (per un commento, invece, di carattere molto analitico a ognuno di essi, si rinvia a E. Goitein, *Another Bite out of Katz: Foreign Intelligence Surveillance and the Incidental Overhear Doctrine*, cit., 112 ss.), si possono sinteticamente ricostruire gli orientamenti su ciascuna delle due questioni.

In linea generale, in tutti i casi citati, il governo argomenta la legittimità della sorveglianza *ex* sez. 702 FISA, benché in assenza di specifici *warrants*, in base ad una serie di considerazioni. In primo luogo, il Quarto Emendamento non si applica ai cittadini stranieri su suolo non statunitense: per questo motivo, nei loro confronti, il problema della sorveglianza *warrantless* neppure deve essere posto. In secondo luogo, benché i cittadini americani vengono "accidentalmente" intercettati, anche nei loro confronti la mancanza di *warrant* si legittima in base a due interpretazioni alternative. Da un lato, si può ritenere che, nel momento in cui questi soggetti comunicano con stranieri, in base alla *third-party doctrine* non sono più detentori di una legittima aspettativa di *privacy* delle loro comunicazioni, poiché, scelgono consapevolmente di relazionarsi con soggetti ai quali il Quarto Emendamento non risulta applicabile. Dall'altro lato, e in subordine, nei casi esaminati, il governo sostiene che, in ogni caso, si stabilirebbe un'eccezione al requisito del *warrant*, denominata "*foreign intelligence exception*" e motivata sulla prevalenza dell'interesse della sicurezza nazionale, da garantire tramite le operazioni di *intelligence*. Nelle tre decisioni citate, le corti hanno accolto l'argomento secondo cui il Quarto Emendamento non si applica agli stranieri, mentre sono state più caute in relazione alla seconda questione. In particolare, pur non spingendosi ad accettare l'argomentazione del governo secondo la quale anche il cittadino americano "vittima collaterale" della sorveglianza non sarebbe più coperto dal Quarto Emendamento, hanno elaborato la c.d. *incidental overhear rule*. In base a questa teoria, si assume che il soggetto statunitense, poiché si interfaccia consapevolmente con un interlocutore straniero, veda la sua aspettativa di *privacy*, se non totalmente annullata, sensibilmente diminuita, tanto da soccombere all'«indisputably compelling» interesse governativo ad attuare il programma di sorveglianza a fini di difesa della sicurezza nazionale (in questi termini, *United States v. Hasbajrami*, cit., 10-13).

In ultima analisi, dunque, si può dire che la sez. 702 del FISA, nonostante sia formulata per applicarsi ai cittadini stranieri, erode in maniera rilevante – con il sostanziale avallo della giurisprudenza – anche le garanzie di *privacy* proprie dei cittadini americani, che risultano cedere di fronte alle ragioni, ritenute indiscutibilmente prevalenti o comunque preponderanti, dettate dalla necessità di tutelare la sicurezza nazionale.

4. – Si presenta, quindi, nei termini appena ricordati il quadro legislativo e giurisprudenziale statunitense alla fine del 2017, quando il regime stabilito dalla sez. 702 FISA sta per giungere a termine. In tale frangente, va rilevato che la proposta, che poi diverrà legge con il nome di *FISA Amendments Reauthorization Act*, non è l'unica pendente dinanzi al Congresso americano. Al contrario, vi sono ben cinque progetti di legge, alcune dei quali tentano di cogliere l'occasione della scadenza del FISA per riformare la normativa in senso maggiormente garantista (v. Congressional Research Service, *Summary of the Substantive Provisions of S. 2010, the FISA Amendments Reauthorization Act of 2017, and H.R. 3989, the USA Liberty Act of 2017*, Nov. 16, 2017, reperibile in fas.org/sgp/crs/intel/fisa-reauth.pdf; S. Hennessey, B. Wittes, *Don't Reform Section 702 Just for the Sake of Reform*, in *Lawfare*, Oct. 16, 2017, reperibile in www.lawfareblog.com/dont-reform-section-702-just-sake-reform), che vengono però accantonate.

Il progetto di legge relativo al *FISA Amendments Reauthorization Act* viene introdotto il 25 ottobre 2017 dal senatore repubblicano Richard Burr. Il testo, approvato l'11 gennaio 2018, è firmato dal Presidente Trump il 19 gennaio 2018. È necessario, a tal punto, esaminare in maniera più analitica i contenuti principali di questa legge.

In primo luogo, secondo la sez. 101 della normativa in questione, l'*Attorney General* e il direttore della *National Intelligence* devono porre in essere procedure «consistent with the requirements of the Fourth Amendment», al momento di interrogare i *databases* contenenti le informazioni raccolte *ex* sez. 702 FISA. Questa norma si riferisce ai casi in cui vengano in rilievo informazioni afferenti a cittadini americani – i soli ai quali il Quarto Emendamento si applica –, ma lo fa in maniera piuttosto vaga e generica, senza specificare le relative procedure. Più puntuale è invece il requisito secondo cui, al fine di accedere ai contenuti di tali comunicazioni, le agenzie di *intelligence* debbano ottenere l'autorizzazione di una corte (*court order*), in caso di «predicated investigations» non correlate con questioni di sicurezza nazionale o con attività di «foreign intelligence». Tuttavia, come notato nei primi commenti alla legge (Brennan Center for Justice, *Vote "No" on Cloture – S. 139 (FISA Amendment Reauthorization Act)*, Jan. 12, 2018, reperibile in www.brennancenter.org), il termine *predicated* indica un'indagine penale arrivata ad uno stadio avanzato. Pertanto, nei passaggi precedenti, i servizi di *intelligence* sono paradossalmente liberi di porre in essere misure di sorveglianza in maniera illimitata, anche relativamente a comunicazioni che potrebbero non essere correlate con la sicurezza nazionale e con operazioni di *intelligence* in territorio estero (tali distorsioni vengono denominate, nel lessico tecnico americano, *backdoor searches*). Per questo motivo, l'inserimento del limite in parola appare surrettizio e facilmente aggirabile, soprattutto se si tiene conto del fatto che la nozione di "sicurezza nazionale" e quella di *foreign intelligence* sono tradizionalmente interpretate in maniera particolarmente ampia e, dunque, appaiono piuttosto rari i casi di operazioni condotte sulla base del FISA in cui esse non vengano in rilievo.

La sez. 102(A) del *FISA Amendment Reauthorization Act*, invece, si sofferma sull'utilizzo processuale delle informazioni ottenute grazie alle tecniche di sorveglianza *ex* sez. 702 FISA. Qualora si tratti di dati relativi a cittadini americani, essi sono utilizzabili come prove solo qualora il governo ottenga un *court order* in tal senso, oppure, in mancanza di esso, il processo penale riguardi una serie tassativa di fattispecie particolarmente gravi. Tuttavia, la qualificazione del processo come afferente a tali seri crimini – fra i quali sono inclusi terrorismo, criminalità transnazionale, reati contro la *cybersecurity* – viene determinata dall'*Attorney General* ed essa non è suscettibile di alcun tipo di *judicial review*. Anche in questo caso, un disposto particolarmente ampio della norma – sebbene celato sotto la garanzia della tassatività delle fattispecie – presenta alte probabilità di aprire ad abusi.

La sez. 102(B) del *FISA Amendment Reauthorization Act*, poi, fa riferimento ad alcuni «reporting requirements», così da imporre ai servizi segreti di pubblicare i dati afferenti al numero di indagini aperte in base a informazioni raccolte *ex* sez. 702 FISA.

La sez. 103 pone, probabilmente, lo snodo più problematico in relazione all'intero atto legislativo. Essa disciplina la c.d. *about collection*. Si tratta della raccolta di dati che non riguardano comunicazioni provenienti *da* o dirette *al target* delle misure di sorveglianza, bensì *riguardano* tale soggetto. Siffatti scambi di informazioni intercorrono, dunque, tra individui diversi che si limitano a menzionare la persona sottoposta a sorveglianza o magari a parlare delle sue attività. In relazione a questo tema, la legge in questione impone, di nuovo, limiti piuttosto inconsistenti, che hanno l'effetto pratico di legittimare il ricorso alla *about collection* – la quale, lo si sottolinea, fino a questo momento era emersa solo come prassi, non ricevendo esplicito riconoscimento normativo. Infatti, si prevede che l'*Attorney General*, almeno trenta giorni prima di autorizzare tale pratica, sia tenuto a darne notizia al Congresso. Tuttavia, non sembra trattarsi di una garanzia particolarmente efficace. In effetti, il Congresso non ha il potere di impedire, direttamente e in ogni singolo caso di specie, la messa in atto di questo tipo di misure; potrebbe farlo, invero, qualora approvasse, nell'ambito della propria discrezionalità, una legge tesa a proibire in via generale la pratica della *about collection*. Nondimeno, è altamente improbabile l'approvazione di una legge nell'arco di trenta giorni e, soprattutto, appare piuttosto inverosimile che ciò accada subito dopo l'entrata in vigore del *FISA Amendment Reauthorization Act*, tramite il quale, se ve ne fosse stata la volontà politica, si sarebbe già potuto mettere fine alla prassi esaminata.

La sez. 104 del *FISA Amendment Reauthorization Act*, inoltre, riguarda le c.d. *minimization procedures*. Si tratta di procedure specifiche di carattere tecnico, che l'*Attorney General* è tenuto ad adottare al fine di evitare il più possibile la diffusione delle informazioni concernenti l'interlocutore statunitense del *target* straniero. Naturalmente, tali accorgimenti giocano un ruolo chiave nella tutela dei cittadini americani, con potenziali riflessi anche, a livello giurisdizionale, sulla configurazione della *incidental overhear doctrine*. La sez. 104 si limita a prevedere che le tecniche di *minimization* debbano essere rese pubbliche dalle agenzie di *intelligence* e dall'*Attorney General* per mezzo di un *report* a cadenza annuale.

5. – Con l'estensione, per i prossimi sei anni, della sez. 702 FISA, gli Stati Uniti non solo confermano l'approccio, da sempre particolarmente permissivo, nei confronti delle limitazioni del diritto alla *privacy* sulla base di vari interessi confliggenti, ma addirittura affievoliscono ulteriormente le relative garanzie nel caso in cui venga in gioco la sorveglianza di cittadini stranieri. Da un lato, questa tendenza impatta sul versante del diritto interno statunitense, in quanto va incidentalmente a diminuire, come si è visto, anche i diritti degli stessi americani che comunicano con i *target* stranieri. Dall'altro lato, dato che spesso i *target* non americani delle misure predisposte dal governo statunitense risultano essere cittadini europei, non si può omettere di considerare la questione anche dalla prospettiva europea. Tanto il livello sovranazionale (Unione Europea, Consiglio d'Europa) quanto quello nazionale (le normative interne dei singoli Stati) offrono infatti un ampio novero di garanzie. Anzi, non ci si può esimere dal richiamare il crescente sforzo della Corte di giustizia dell'Unione europea nel bilanciare *privacy* e *data protection* con le esigenze della sicurezza nazionale, andando anche al di là del mero dato normativo e impegnandosi nella costruzione di un quadro giuridico di tutela di questi diritti che possa dirsi avere carattere transfrontaliero. La Corte di Lussemburgo, infatti, da ultimo con il parere 1/15 del 26 luglio 2017, relativo allo scambio di dati PNR tra paesi dell'Unione e Canada e potenzialmente foriero di implicazioni anche per i rapporti con gli Stati Uniti (per un'approfondita analisi, si rinvia ad A. Vedaschi, *Privacy and data protection versus national security in transnational flights: the EU-Canada PNR agreement*, in corso di pubblicazione in *International Data Privacy Law*, 2018), ma anche nella precedente giurisprudenza, si è sforzata di estendere addirittura al di là dei confini territoriali dell'Unione gli *standard* in materia di *privacy* e *data protection*. La chiave di volta per tale estensione è il requisito dell'«adequate level of protection» dei dati personali, richiesto dal

diritto UE a qualsiasi paese intenda scambiare dati con gli Stati membri dell'Unione. È poi d'uopo, spostandosi sul livello legislativo, richiamare la nuova disciplina normativa in tema di *data protection*, fissata dal nuovo *General Data Protection Regulation* (Regolamento (UE) 2016/679) e da due direttive (Direttiva (UE) 2016/680 e Direttiva (UE) 2016/681), relative alla protezione dei dati personali nell'ambito della lotta al crimine e dell'esecuzione delle sanzioni penali, la prima, e all'uso dei dati PNR, la seconda.

Si crea un'inevitabile tensione, quindi, tra la crescente richiesta di tutela sul versante europeo e il quadro giuridico statunitense, la cui tendenza va inesorabilmente verso un notevole "ribasso" delle stesse garanzie. Tale tensione non giova certo alla fittissima rete di relazioni commerciali e strategiche che intercorre tra i due attori in questione e, per questo motivo, nel prossimo futuro si potrebbe assistere ad un'ulteriore espansione del ruolo (già cruciale) di strumenti quali accordi internazionali e convenzioni tra la parte europea e quella statunitense, che ambiscano a comporre, almeno in parte, il rilevante *gap* tra i rispettivi *standard* di protezione.