Costituzionalismo.it

Fascicolo 2 | 2015
I DIRITTI DEI DETENUTI

ACLU v. Clapper: una nuova stagione per il right to privacy?

di MARIAVITTORIA CATANZARITI

ACLU v. Clapper: una nuova stagione per il right to privacy?

di MARIAVITTORIA CATANZARITI
Dottore di ricerca in Filosofia del diritto - Università degli Studi "Roma Tre"

Il presente scritto esamina la pronuncia ACLU v. Clapper del Second Circuit dello scorso 7 maggio 2015, la quale ha dichiarato l'illegittimità del "Bulk Telephony Collection Program" per eccesso di limiti previsti dal § 215 FISA. Sebbene la pronuncia accolga le sole censure fondate sulla contrarietà alle norme di legge, essa percorre alcuni passaggi fondamentali dell'evoluzione del concetto di privacy nell'era della sorveglianza elettronica.

This paper examines the recent case ACLU v. Clapper, decided by the Second Circuit on the 7th May 2015, which held that the "Bulk Telephony Collection Program" was illegitimate under § 215 FISA. The judgment mostly focused on statutory claims.
However, the decision seems to be even more important since the arguments adopted highlight a changing appreciation of the importance of the right to privacy in the surveillance society.

Il contesto di riferimento

Una recente pronuncia dello scorso 7 maggio della US Court of Appeals, Second Circuit[1], potrebbe mutare sensibilmente gli orizzonti dell'attuale dibattito sulla sorveglianza elettronica negli Stati Uniti[2].

Si tratta di una decisione che, ribaltando le conclusioni raggiunte dalla sentenza di primo grado[3], ha dichiarato l'invalidità del programma di intercettazioni telefoniche di massa - il cosiddetto "Bulk Telephony Collection Program" – posto in essere dalla National Security Agency (NSA) per contrarietà ai dettami legislativi e costituzionali dell'ordinamento statunitense[4]. Preliminarmente all'analisi della sentenza, si tracceranno le caratteristiche generali del quadro di riferimento entro il quale s'inscrive la controversia in oggetto[5].

Il programma di sorveglianza in questione, autorizzato dal Governo americano in conformità alla versione originaria del § 215 Foreign Intelligence Surveillance Act (FISA)[6], consente al Direttore del Foreign Bureau of Investigation (FBI) di richiedere alla Foreign Intelligence Surveillance Court (FISC) l'emissione di un decreto volto a ottenere la produzione di "tangible things" nell'ambito di indagini di *foreign intelligence*. Tali indagini devono perseguire finalità di lotta al terrorismo o ad attività clandestine di *intelligence*, ma non possono riguardare cittadini statunitensi. Il programma prevede che i dati rimangano a disposizione della NSA per un periodo massimo di cinque anni[7].

Detto programma, era stato autorizzato per la prima volta da un decreto della FISC del 24 maggio 2006 – il cosiddetto FISC "*Primary order*" – indirizzato alla compagnia telefonica *Verizon*. Tale decreto, il quale era coperto dal vincolo del segreto, imponeva a *Verizon* il trasferimento alla NSA su base quotidiana dei metadati e di tutti i dati telefonici – ad eccezione dei contenuti vocali delle

conversazioni - riguardanti le comunicazioni in entrata o in uscita dagli Stati Uniti o interne al territorio americano. I metadati erano stati analizzati mediante l'uso dei cosiddetti "selectors" e "trunk identifiers", in grado di rivelare informazioni generali sulla localizzazione degli utenti, mediante l'associazione ai dati telefonici raccolti. L'utilizzazione dei metadati da parte della NSA presuppone l'inserimento del numero telefonico all'interno di un *database*, ovvero dell'*identifier* associato ad un'organizzazione terroristica sospetta. Secondo le norme di legge, tuttavia, l'*identifier* non può tuttavia essere utilizzato per estrapolare dati, qualora questi attengano esclusivamente ad attività coperte dal Primo Emendamento[8], quali ad esempio la libertà di manifestazione del pensiero. Il ricorso a un *identifier* quale strumento di interrogazione del sistema – tecnicamente noto come "seed" – deve essere approvato da uno dei ventidue funzionari della NSA sulla base di un "reasonable, articulable suspicion" (RAS).

Dopo le rivelazioni di Edward Snowden e la divulgazione sugli organi di stampa il 5 giugno 2013 di un analogo decreto FISC (cosiddetto *Secondary order*), anch'esso protetto da segreto[9], il Governo statunitense riconobbe pubblicamente di aver raccolto sin dal maggio 2006 i dati relativi a tutte le conversazioni telefoniche effettuate all'interno degli Stati Uniti, incluse le telefonate tra Stati Uniti e paesi stranieri. Esso confermò, altresì, la legittimità del decreto che ingiungeva alle compagnie telefoniche il trasferimento di "any tangible things" alla luce del § 215 FISA. Il *Secondary Order* non fu altro che una reiterazione del *Primary Order* del 2006. E' interessante osservare che dal 2006 il termine di validità del *Primary order* (generalmente di 90 giorni) è stato ripetutamente prorogato circa quaranta volte[10]. Nel 2006 il Congresso ha anche apportato un emendamento al § 215, prevedendo che al Governo dovesse essere richiesto uno "statement of facts" comprovante la presenza di fondati motivi idonei a far ritenere che le suddette "tangible things" fossero rilevanti ai fini di un'"authorized investigation"[11], nonché un'enumerazione delle "minimization procedures".

Tra queste ultime, se ne possono annoverare alcune, come ad esempio l'obbligo per la NSA di trattamento dei dati in network a circuito chiuso e per le sole finalità legittime in conformità al FISC; la distruzione dei dati dopo cinque anni dalla raccolta; la competenza esclusiva dei ventidue funzionari NSA per quanto riguarda la determinazione del RAS; il divieto di divulgazione dei risultati ottenuti mediante l'interrogazione del sistema se non in conformità alle

procedure FISC, fatta eccezione per i casi in cui almeno uno tra i cinque funzionari di alto rango ne affermi la rilevanza per le finalità di lotta al terrorismo; la messa a punto di sistemi di tecnologia e formazione di personale specializzato tali da assicurare che le interrogazioni siano effettuate con riferimento a *identifiers* che giustifichino la "reasonable, articulable suspicion"; la sottoposizione del programma al doppio controllo interno ed esterno, sia da parte del FISC sia da parte dell'Intelligence and Judiciary Committee [12].
Tuttavia, come si avrà modo di approfondire in seguito, per effetto della pronuncia in commento, il FISC *order* dovrà d'ora in poi specificamente autorizzare ciascuna nuova ipotesi di raccolta in blocco dei metadati ai sensi del § 215 FISA, non potendo limitarsi a una semplice reiterazione dei precedenti decreti.

In seguito alla rivelazione pubblica dei programmi di sorveglianza elettronica di massa, il Presidente Obama, nel gennaio 2014, ha apportato alcune modifiche alla procedura autorizzata dal FISC *order* del 5 febbraio 2014[13]: la prima riguardava il divieto di interrogazioni del sistema mediante l'uso dei "selectors" associati ai "seeds" per più di due volte ("second hop"); la seconda consisteva nella necessità che la sussistenza di "reasonable ground" fosse attestata dalla FISC stessa e non invece, come era stato finora, da parte di funzionari della NSA. Queste modifiche sono state il frutto del dibattito pubblico originato dal cosiddetto "NSA scandal" e dalla pubblicazione dei rapporti tematici del Review Group on Intelligence and Communications Technologies e del Privacy and Civil Liberties Oversight Board (PCLOB)[14].

Invero, occorre precisare che esistono due forme di controllo giurisdizionale del NSA *program*: il primo è il FISC *order* autorizzato a norma del § 215 FISA, del quale ci siamo sin qui occupati; il secondo è il controllo giurisdizionale ordinario attribuito alle corti federali dall'art. 3 della Costituzione statunitense[15]. Quanto a quest'ultimo va precisato che la valutazione dello "standing" è particolarmente rigorosa e si richiede che il pregiudizio fatto valere dal ricorrente sia "concrete, particularized, and actual or imminent"[16]. Sin qui è da rilevare la tendenza restrittiva delle corti ordinarie soprattutto in ordine alla considerazione dell'analisi del merito del ricorso. La dottrina dello *state secret privilege*, in particolare, ha rappresentato l'ostacolo più rilevante, in quanto l'impossibilità da parte del ricorrente di accedere alle notizie coperte da segreto ha reso quanto mai difficile esaudire l'onere della prova, determinando per lo

più il rigetto dei ricorsi[17].

La controversia

La decisione del Second Circuit si colloca all'interno di un lungo filone giurisprudenziale, inaugurato con il caso *United States v. U.S. Dist. Court for the Eastern District of Michigan*, deciso dalla Corte Suprema nel 1972[18]. All'interno di questo filone ai fini dell'analisi della pronuncia in esame, assumono particolare rilevanza due casi specifici: *Amnesty International v. Clapper**[19]*; *ACLU v. Clapper**[20]*.

Il primo, deciso poco prima delle rivelazioni di Snowden, è un chiaro esempio di come gli stringenti requisiti attinenti alla legittimazione processuale rispetto alle controversie promosse di fronte alle corti federali ex art. 3 della Costituzione federale comportino spesso un ostacolo alla tutela. Gli attori erano tra gli altri, avvocati, organizzazioni umanitarie no-profit e giornalisti, i quali lamentavano il fatto di essere stati pregiudicati nella libertà di comunicare con i propri interlocutori a causa della costante sorveglianza del traffico telefonico e telematico operata dalla NSA. In particolare tali attività rientravano all'interno di un programma in ragione del quale erano state intercettate telefonate e email, tra le quali quelle dei ricorrenti, quando una parte si trovava al di fuori del territorio statunitense e un partecipante alla conversazione era ragionevolmente sospettato di essere un membro o un agente di *al Qaeda* ovvero di un'organizzazione terroristica ad essa affiliata. La Corte rigettò il ricorso per insussistenza di *standing*, in quanto esso non poteva ritenersi fondato soltanto sulla base di un timore di danno ipotetico e non attuale.

Nel caso ACLU v. *Clapper*, arrivato in appello, invece, sia la Corte di primo grado, sia la Corte d'Appello, ritennero sussistente lo *standing,* poiché la raccolta dei metadati da parte della NSA avrebbe costituito un pregiudizio rilevante, concreto e attuale. La sentenza di primo grado nasceva da un ricorso promosso, tra gli altri, dalla American Civil Liberties Union e dalla New York Civil Liberties Union, nel quale gli attori chiedevano la declaratoria di illegittimità del Bulk Telephony Collection Program e un'inibitoria cautelare (*preliminary*

injunction). La Corte aveva rigettato sia le censure mosse dagli attori in ordine alla costituzionalità del programma attuato dal Congresso sotto il profilo del Primo e del Quarto Emendamento, sia le censure in punto di violazione dei requisiti di legge, ribadendo peraltro pragmaticamente che "the effectiveness of bulk telephony metadata collection cannot seriously be disputed"[21]. In particolare, tra gli *statutory claims* gli attori lamentavano la mancanza di copertura legislativa del programma di raccolta di metadati telefonici sotto il § 215 FISA. Gli attori erano stati, sia pure in maniera diversa, clienti della società *Verizon* e affermavano che le loro conversazioni fossero state intercettate in assenza di uno specifico mandato in base al *Secondary order*. La Corte, nel rigettare le censure mosse nei confronti del programma, attribuì notevole rilevanza alla *third party doctrine*. In base a tale dottrina, che ricevette un espresso sugello formale nel noto caso *Smith v. Maryland**[22]*, gli individui non possono vantare una legittima aspettativa di *privacy,* rilevante ai sensi del Quarto Emendamento della Costituzione Federale, riguardo alle informazioni che essi stessi trasferiscono a terzi in maniera volontaria. Pertanto, i dati in possesso della compagnia telefonica non avrebbero goduto delle garanzie costituzionali, in quanto volontariamente trasmessi dai ricorrenti alla compagnia telefonica mediante la digitalizzazione dei numeri telefonici. Nel caso *Clapper* la Corte ritenne inapplicabile il precedente *United States v. Jones* della Corte Suprema[23] , nel quale quest'ultima aveva dichiarato che l'istallazione di un GPS all'interno di una macchina di un presunto terrorista per il periodo di 28 giorni consecutivi avesse comportato una violazione del Quarto Emendamento. In tal caso, dunque, la *third party doctrine* non veniva in rilievo, in quanto mancava l'elemento della trasmissione volontaria dei dati a terzi. Nel ritenere applicabile la *third party doctrine* al caso *Clapper*, la Corte richiamò invece il caso *Katz v. United States**[24]*, nel quale la Corte aveva sostenuto che l'istallazione di un *pen register* non costituisse un "search" rilevante quale violazione del Quarto Emendamento. Ciò in quanto gli individui che effettuano chiamate trasmettono i numeri di telefono alle compagnie telefoniche e implicitamente assumono il rischio che la compagnia riveli alla polizia i numeri selezionati.

La District Court ritenne che il ragionamento svolto in *Smith* potesse essere applicato, *mutatis mutandis* alle intercettazioni di massa, anche in base all'orientamento espresso da diverse altre corti negli anni '80 e '90. Va notato comunque che nel caso *Jones*, la violazione del Quarto Emendamento fu affermata pur sempre in ragione di un "physical trespass" all'interno di una

sfera costituzionalmente protetta, ossia un'automobile, ma la sentenza non affrontò la questione della violazione del Quarto Emendamento in mancanza di un "physical trespass"[25]. Emblematica in detta sentenza fu l'opinione concorrente di Justice Sotomayor, la quale sostenne che attività di sorveglianza di così lunga durata come quelle realizzate per il periodo di 28 giorni attraverso l'utilizzo del *pen register*, fossero tali da rivelare una mole enorme di dati sulla famiglia, sulle inclinazioni politiche, religiose e sessuali. In conclusione, Justice Sotomayor ritenne che la *third party doctrine* fosse ormai datata rispetto allo sviluppo tecnologico[26].

In effetti, la questione fondamentale del caso *Clapper*, e il mutamento di prospettiva evidenziato nel passaggio dal primo al secondo grado, consiste proprio nell'applicabilità o meno della *third party doctrine* alle fattispecie di sorveglianza elettronica[27]. In particolare, mentre la corte distrettuale aveva negato sin da principio l'inerenza della *third party doctrine* al caso in esame, la corte d'appello lasciava intendere, pur non analizzando nel merito le censure costituzionali, il carattere anacronistico di detta dottrina se applicata alle attività di sorveglianza elettronica.

La District Court considerava la creazione e la conservazione dei "business records" di pertinenza della compagnia telefonica *Verizon*, rigettando dunque le censure di costituzionalità relative alla violazione del Quarto Emendamento [28]. Inoltre Justice Pauley, estensore della sentenza di primo grado, aveva sostenuto che il tipo di informazioni contenute nei metadati fosse limitato e che, pertanto, non fosse idoneo a costituire un "search" a norma del Quarto Emendamento. Riprendendo la sentenza *Amnesty International v. Clapper*, non ritenne, infatti, sussistente lo *standing* degli attori alla luce del parametro della "objectively reasonable likelihood", essendo il ricorso fondato, secondo la Corte, su un timore di danno meramente astratto[29]. Nel merito, egli rilevò che la parte attrice non avesse fornito prova sufficiente della ragionevole probabilità di prevalere in punto di violazione delle norme di legge, né della presenza dei requisiti richiesti per l'ottenimento di un *preliminary injunction* (tra i quali il rischio di pregiudizio irreparabile, prova del pubblico interesse, etc.) [30].

Inoltre, con riferimento alla violazione del Primo Emendamento, i ricorrenti lamentavano la produzione di un "chilling effect" rispetto alle relazioni che si

sarebbero potute stabilire con potenziali utenti, e dunque invocavano l'esistenza di un pregiudizio rispetto alla libertà di associazione e comunicazione. Justice Pauley riprese le conclusioni raggiunte in *Clapper v. Amnesty International*, ribadendo che il solo astratto timore di un pregiudizio non potesse integrare una violazione del Primo Emendamento[31].

In conclusione, il giudice non soltanto affermò la piena costituzionalità del programma, ma aggiunse che il § 215 FISA avrebbe implicitamente precluso qualsiasi forma di controllo giurisdizionale.

La decisione della Corte Federale d'Appello

Lo schema interpretativo del Second Circuit ruota innanzitutto intorno al problema della legittimazione ad agire in base al Quarto Emendamento. Uno dei precedenti più significativi in materia è rappresentato da *United States v. Verdugo-Urquidez**[32]*, secondo il quale sussiste una violazione del Quarto Emendamento ogni qualvolta vi sia una irragionevole intrusione da parte del governo nella sfera privata dell'individuo. Ora, secondo la Corte, nel caso *Clapper*, il fatto che l'intrusione avvenga mediante un dispositivo elettronico, e segnatamente mediante l'interrogazione individualizzata del database contenente i metadati, non è sufficiente a privare i ricorrenti della legittimazione ad agire.

Gli attori lamentavano l'abuso di potere da parte della NSA per violazione dell'APA (Administrative Procedure Act). In base a quanto disposto dal § 702 dell' APA, una persona, che abbia subito un illecito derivante da attività della pubblica amministrazione, può citare in giudizio gli Stati Uniti per ottenere un "relief other than money damages".

Tuttavia il § 223 Patriot Act, riformando nel 2006 il Wiretap Act e lo Stored Communication Act, aveva eliminato la possibilità di citare in giudizio il Governo Americano per le violazioni concernenti detti provvedimenti, e ristretto fortemente l'accesso alle corti per i casi previsti al di fuori di essi. Inoltre, tale disposizione aveva introdotto l'azione di danni quale rimedio esclusivo per

violazioni volontarie del Wiretap Act e dello Stored Communication Act e di tre disposizioni del FISA riguardanti le seguenti attività: *electronic wiretap surveillance*, *physical searches* e *pen registers* o *trap and trace devices**[33]***.

Muovendo da tali premesse, il Governo portava avanti due linee argomentative: la prima riguardava l' insussistenza dello *standing* da parte degli appellanti - tuttavia affermata dalla Corte - nel dimostrare che il danno subito mediante la raccolta dei metadati per violazione del Primo e del Quarto Emendamento fosse stata "certainly inpending", requisito peraltro richiesto anche nel precedente *Amnesty International v. Clapper**[34]*** e non integrato in quel caso secondo la Corte Suprema; la seconda riguardava per l'appunto la cosiddetta "preclusion", cioè la presunta impossibilità di impugnare gli atti governativi ricompresi nell'ambito del § 215 FISA da parte di soggetti diversi dalle compagnie telefoniche destinatarie del FISC *order*.

A tal proposito, il § 223 Patriot Act, nel prevedere quale rimedio esclusivo detta azione di danni, non faceva menzione del § 215. Ciò, a parere del Governo, significava aver intenzionalmente escluso il § 215 dall'ambito di applicazione della norma, con la conseguenza che il Congresso non avrebbe inteso sottoporre gli atti amministrativi coperti dal § 215 al controllo giurisdizionale[35].

Al contrario, l'argomento degli appellanti muoveva proprio dalla mancanza di un riferimento normativo al § 215, necessario, secondo la tesi difensiva di costoro, a far sì che sulle materie coperte da detta disposizione potesse essere escluso il controllo giurisdizionale ordinario e fosse garantita al più la sola azione di danni.

Per la Corte, dunque, il nodo da dirimere consisteva nello stabilire se il Governo avesse, o meno, fornito sufficiente prova che il Congresso intendesse precludere il controllo giurisdizionale. La Corte analizzava pertanto la questione sotto i seguenti profili: il primo riguardava il carattere segreto che coinvolge tutte le attività connesse al § 215. Il secondo era incentrato su un rilievo fattuale, e cioè che il § 215 non potrebbe sostanzialmente essere efficace se fosse soggetto a controllo giurisdizionale o se fosse limitato, in quanto esso può ricevere un'effettiva applicazione soltanto attraverso una raccolta indifferenziata di tutti i dati (cosiddetto "blunt tool")[36]. Il terzo consisteva nel fatto che il Congresso avrebbe avuto varie volte occasione di approvare un emendamento tale da precludere l'impugnazione dei FISC *order* dinanzi alle corti federali. Infine l'argomento residuale, e tuttavia non poco incisivo, consisteva nell'affermare in

ogni caso la possibilità di agire per violazione dei diritti costituzionali di cui al Primo e al Quarto Emendamento.

Gli appellanti sostenevano, al contrario, che sarebbe stato necessario escludere espressamente il § 215 dall'ambito di applicazione del § 223 Patriot Act, per far sì che l'azione di danni fosse preclusa anche nei casi ricompresi del § 215 FISA. Essi facevano leva sulla storia legislativa degli emendamenti del § 215, che avevano portato all'aggiunta di una previsione del controllo giurisdizionale di portata generale, peraltro esteso anche alle *national security letters* [37].

Secondo la Corte, il fatto che il § 223 non contenesse specificamente un richiamo negativo al § 215 avvalorava la tesi degli appellanti. Il § 223 non doveva applicarsi, dunque, secondo la Corte, al § 215, non nel senso che in quest'ultimo caso il rimedio esclusivo sarebbe stato l'azione di danni, ma nel senso che non facendo menzione del § 215, il § 223 non avrebbe precluso il controllo giurisdizionale *tout court*. La Corte concludeva, pertanto, nel senso che il Congresso avrebbe dovuto prevedere una specifica esenzione del § 215 dal controllo giurisdizionale, rigettando così gli argomenti presentati dal Governo. Gli appellanti avevano, pertanto, diritto di azione in base all'APA e dunque, secondo la Corte, poteva procedersi nell'analisi del merito.

Vi è da osservare che, sebbene i ricorrenti lamentassero la violazione dei parametri costituzionali, e specificamente, il fatto che l'autorizzazione da parte del Congresso di detti ordini fosse stata resa in violazione del Quarto Emendamento, il primo motivo di ricorso verteva di fatto sulla sola mancanza di copertura legislativa di detti programmi in base alla norma alla quale il Governo faceva riferimento come base giuridica del programma di intercettazioni di massa. In particolare, i ricorrenti rilevavano che molte delle registrazioni raccolte non fossero direttamente utilizzabili per finalità investigative. Nell'adozione del § 215 FISA, infatti, il Congresso aveva attribuito al Governo un amplissimo potere investigativo, funzionale, secondo le conclusioni del Governo stesso, per le finalità di antiterrorismo. I ricorrenti contestavano specificamente il fatto che la raccolta prolungata negli anni di metadati fosse rilevante per dette finalità.

Il Governo, di contro, sosteneva che la raccolta di metadati, benché non immediatamente rilevante in sé e per sé, fosse tuttavia utile per identificare altre informazioni rilevanti mediante l'uso dei "selectors". Esso sosteneva, ancora, che il Congresso avesse fatto propria la suddetta lettura del § 215 mediante la

sua riattuazione senza modifiche sia nel 2010 sia nel 2011. Ogni sei mesi il Governo ha, infatti, l'obbligo di riferire ai comitati giudiziari e di intelligence della Camera e del Senato su qualsiasi interpretazione del FISC riguardante il §215. Peraltro nel 2010 e nel 2011 venne reso noto un documento riservato sul *Bulk Telephony Program* che manteneva sostanzialmente immutato il § 215. Da ciò la Corte ha tratto un ulteriore elemento per affermare che il Congresso avrebbe sostanzialmente ratificato l'interpretazione del § 215 data dal Governo[38].

Vi è da osservare, del resto, che il Governo non ha finora reso noti i presupposti in base ai quali la raccolta di metadati fosse rilevante per le finalità di un'indagine autorizzata.

In base a tali considerazioni, la corte ha accolto tutte le censure di eccesso di limiti legislativi del § 215.

Per quanto riguarda, invece, la contrarietà del programma al Primo e Quarto Emendamento della Costituzione, i ricorrenti contestavano gli argomenti del Governo sostenendo la necessità di una revisione della *third party doctrine*, sulla base della considerazione che la sorveglianza elettronica rappresentasse un fenomeno senza precedenti, e dunque tale da non poter essere assimilato alle fattispecie tradizionali di violazione della *privacy*[39]. Sul punto il Second Circuit, pur richiamando il ragionamento percorso dalla District Court, riteneva tuttavia non necessario analizzare i profili di censura costituzionale, dal momento che il programma di intercettazioni di massa non aveva avuto neanche la copertura legislativa del §215 FISA[40].

Ciò non significava, secondo la Corte, che la controversia fosse irrilevante sotto il profilo delle censure di costituzionalità. La Corte, tuttavia, affermava espressamente che le suddette potessero essere adeguatamente analizzate soltanto dopo un intervento interpretativo chiarificatore da parte del Congresso sui limiti del concetto di *privacy* e sulla misura in cui la moderna tecnologia potesse alterare la tradizionale aspettativa di *privacy*.

Peraltro la Corte, con la sentenza del 7 maggio scorso, aveva rinviato al primo grado la decisione in merito all'ottenimento di una *preliminary injunction*, dal momento che a breve il Congresso deciderà se autorizzare o meno il programma di intercettazioni di massa sotto la copertura legislativa del § 215.

Potrebbero a quel punto aprirsi due possibili scenari: nel caso in cui il Congresso reiteri l'*order* senza estendere espressamente l'applicazione del § 215 ai metadata telefonici, non vi sarà la necessità di ricorrere a un *prospective relief* una volta concluso il programma. Se invece il Congresso porrà in essere un programma sostanzialmente modificato, vi sarà allora la possibilità per i ricorrenti di sollevare vizi di invalidità costituzionale in termini diversi da quelli prospettati con il presente ricorso. La Corte d'Appello si limita dunque a ritenere che il programma di raccolta dei metadati telefonici ecceda i limiti del § 215 e per questo annulla la decisione della District Court che aveva rigettato il ricorso degli attori, rinviando ad essa per una decisione nel merito. La Corte insiste prevalentemente sul fatto che nelle settimane immediatamente successive alla sentenza sarebbe scaduta l'autorizzazione del § 215 (in data 2 giugno 2015) e che, dunque, la sede più consona per deliberare in merito alla modifica dei termini di autorizzazione del programma sarebbe stata quella politica e non invece quella giudiziaria. In particolare, tale determinazione si assesta proprio sulla valutazione dell'*irreparable harm*, che rappresenta uno dei due presupposti per l'ottenimento della *preliminary injunction*, insieme al *likelihood to succeed in the merits*. Ora, secondo la Corte, mentre sussisterebbe, a differenza di quanto affermato dalla corte di primo grado, l'alta probabilità di prevalere nel merito (essendo la violazione di legge conclamata), il pregiudizio irreparabile invece non risulterebbe integrato in quanto il Congresso avrebbe dovuto decidere a breve sulle modalità di contemperamento degli interessi in gioco, cioè sicurezza e privacy. E difatti il 2 giugno 2015 il Senato ha approvato il Freedom Act[41], con il quale l'attività della NSA è stata fortemente limitata. Tale riforma tocca moltissimi punti relativi alle procedure di sorveglianza elettronica adottate dal Governo statunitense[42], tra i quali assume particolare rilevanza quello relativo ai FISA Business Records. Tale sezione ha emendato le procedure FISA relativi ai FISC *order* richiesti da parte del FBI ed è stata replicata anche a proposito delle National Security Letters, prevedendo l'obbligo per l'FBI di presentare uno "specific selection term" che identifichi il destinatario della raccolta, il dispositivo elettronico, l'indirizzo fisico o elettronico circostanziato o un *account* ai fini della produzione delle "tangible things".

Il nuovo testo fornisce inoltre una definizione del "call detail record" che consiste in una sessione identificativa dei metadati ad eccezione dei contenuti delle comunicazioni, del nome, dell'indirizzo o delle informazioni finanziarie del

cliente e in generale sul sistema di localizzazione globale.

Tra le altre modifiche rilevanti vi è il termine massimo di raccolta di 180 giorni e la possibilità da parte della FISC di nominare cinque individui quali *amicus curiae*, nonché la limitazione del potere dell'Attorney General di derogare alle procedure FISC, ammesso ad esempio soltanto con il correttivo dell'obbligo di informazione tardivo o della richiesta tardiva di un *order*.

La decisione della Corte d'Appello si pone in linea con un precedente di appena dieci giorni successivo alla sentenza *Clapper* di primo grado. Detto precedente, *Klayman v. Obama*, della District Court of the District of Columbia, giungeva a conclusioni completamente diverse dalla sentenza *Clapper* di primo grado. Non soltanto, infatti, in base a detta pronuncia, l'istallazione di un *pen register* veniva considerato una violazione del Quarto Emendamento, ma il precedente Smith non poteva essere applicato al tema della sorveglianza di massa. L'uso della moderna tecnologia, secondo il *reasoning* della District Court of the District of Columbia, avrebbe reso inapplicabile il parametro della "reasonable expectation of privacy" in conformità al Quarto Emendamento[43]. In particolare, Justice Leon considerò ammissibile la richiesta dei ricorrenti di un "preliminary injunction relief" e altamente probabile la possibilità per i ricorrenti di dimostrare che le cosiddette "searches" rilevanti per il Quarto Emendamento, fossero "unreasonable" e "unconstitutional"[44]. La Corte affermò, infatti, che la cultura "telefonocentrica" della società contemporanea rende ormai i metadati potenziali dati sensibili, nella misura in cui essi siano in grado di rivelare "an entire mosaic…a vibrant and constantly updating picture of the person's life"[45]. Ad oggi non vi è ancora stata una pronuncia nel merito sull'incostituzionalità del "bulk telephony metadata program", segno di quanto sia calda e spinosa la questione della sorveglianza di massa negli Stati Uniti[46].

Considerazioni conclusive

La pronuncia del Second Circuit, nonostante rappresenti un positivo segno di

apertura delle corti statunitensi nei confronti della tutela delle libertà civili, considerando anche l'impianto della riforma dell'US Freedom Act che ne consegue, costituisce ancora un timido progresso nell'intricato scenario giuridico americano che vede contrapposti *national security* e *privacy*[47]. Svolgendo alcune considerazioni di sistema, infatti, vi è da osservare che il dibattito statunitense si è notevolmente vivacizzato negli ultimi tempi, virando in favore della limitazione del potere della NSA, anche a seguito della nota pronuncia della Corte di Giustizia che ha annullato la Direttiva 2006/24/CE sul Data Retention[48], e in generale, delle reazioni suscitate in ambito europeo a seguito delle rivelazioni riguardanti l'intercettazione dei cittadini europei da parte del Governo americano[49]. Basti pensare alla serrata attività emendativa e di *advocacy* portata avanti dall'art. 29 Working Party o dal Comitato libertà civili, giustizia e affari interni del Parlamento Europeo (LIBE) riguardo alla proposta di Regolamento Europeo redatta dalla Commissione[50]. E' peraltro recente il rinvio pregiudiziale dell'Alta Corte irlandese nei confronti della Corte di Giustizia in merito alla compatibilità del Safe Harbor Agreement con gli articoli 7 e 8 della Carta dei Diritti Fondamentali dell'Unione Europea [51]. La questione riguarda, nello specifico, la legittimità del trasferimento dei dati da *Facebook* alla NSA alla luce del diritto europeo, in quanto coperto dal *Safe Harbor Agreement*. Anche la Corte Europea è stata recentemente destinataria di un ricorso da parte di una società inglese promotrice delle libertà civili (*Big Brother Watch and Others* v. *UK*[52]), la quale lamentava che il programma inglese di *mass surveillance* "Tempora" fosse stato attuato in violazione dell'art. 8 CEDU. Al momento la Corte non ha ancora emesso una sentenza.

Trattandosi di programmi di sorveglianza di massa che hanno una portata globale, si è assistito difatti a un'operazione di concorrenza culturale tra due ordinamenti giuridici, quello europeo e quello statunitense, i quali presentano due visioni del diritto alla *privacy* completamente diverse[53]. In Europa la *privacy* è, dopotutto, considerata un diritto fondamentale, là dove negli Stati Uniti essa è ancora vista essenzialmente come un diritto dell'individuo contro lo stato[54]. Altro profilo molto complesso, e per nulla trascurabile, attiene ai livelli di tutela nazionale/sovranazionale in Europa e statale/federale negli Stati Uniti. Si percepisce, dunque, un tentativo reciproco di accorciare le distanze culturali attraverso un'accelerazione nella previsione dei rimedi, in gran parte giudiziari e legislativi, in risposta tuttavia alla concorrenza nei fini dei diversi programmi di sorveglianza. Va da sé che risulta notevolmente alterato il senso

della cultura giuridica che fonda determinate scelte di sistema, le quali appaiono per lo più dettate dall'equiparazione di *standard* di tutela più che da scelte politiche consapevoli.

Tuttavia, nonostante i notevoli progressi nel tentativo di porre un freno alle pratiche illegali di sorveglianza, i nodi cruciali rischiano di essere sottaciuti nella valutazione ultima dei rimedi offerti dai modelli giuridici americano ed europeo. Mi riferisco, in particolare, a due problemi estremamente rilevanti, che non hanno trovato spazio né nel testo del US Freedom Act né nella bozza del Regolamento Europeo Data Privacy: il primo attiene alla segretezza delle procedure di sorveglianza elettronica, baluardo indefettibile tanto del vecchio stato nazione quanto delle più avanzate forme di democrazia[55]; il secondo attiene ai limiti della extraterritorialità delle corti[56].

A mero titolo esemplificativo, infatti, sino a quando sarà estremamente oneroso dar prova delle violazioni dei diritti individuali derivanti dai programmi di intercettazione di massa, a causa della segretezza delle procedure alle quali essi sono sottoposti, ovvero fino a quando sarà precluso l'accesso alle corti americane per i cittadini europei vittime di intercettazioni di massa da parte della NSA al di fuori del territorio statunitense (e viceversa) [57], qualsiasi analisi risulterà depotenziata dalla parzialità degli orizzonti.

Un annoso dilemma, quello della nave di Teseo: nave nuova con vecchie tavole o vecchia nave con tavole nuove.

[1] *ACLU v. Clapper*, V. 14 - 42, Document 168-1, 1503586 (2d Cir. 05/07/2015).

[2] Cfr. Neil M. Richards, *The Dangers of Surveillance*, Harward Law Review, Vol. 126, p. 1934; Neil M. Richards - Jonathan H. King, *Big Data Ethics*, Vol. 49, 2014, p. 393; *Three Paradoxes of Big Data*, Stanford Law Review Online, Vol. 67, 2013, p. 41; Kate Krawford – Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, Boston College Law Review, Vol. 55, 2013, p. 93.

[3] *ACLU v. Clapper*, F. Supp. 2d 724 (S.D.N.Y. 27/12/2013).

[4] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, Harward Journal of Law and Public Policy, Vol. 37, 2014, p. 759, 836, 871, 874.

[5] Sul punto cfr. David S. Kris, *On the Bulk Collection of Tangible Things*, Journal of National Security Law & Policy, Vol. 7, 2014, p. 209.

[6] La norma riguardava originariamente i soli "business records", ma fu estesa successivamente, in seguito alle modifiche apportate nel 2008 al § 215 FISA dal Patriot Act, alle cosiddette "tangible things".

[7] *Primary Order*, BR 13-80 (FISA Ct. Apr. 25, 2013).

[8] *ACLU v. Clapper*, F. Supp. 2d 735.

[9] *Secondary Order*, BR 13-80 (FISA Ct. 25/04/2013).

[10] Erin E. Connare, *ACLU v. Clapper: The Fourth Amendment in the Digital Age*, Buffalo Law Review, vol. 63, 2015, p. 397.

[11] § 215 FISA (U.S.C. §1861, b. 2-a).

[12] Erin E. Connare, *op.cit.*, p. 395, 398, 401.

[13] Prod. of Tangible Things, No. BR - 14 - 01.

[14] Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, Stanford Journal of International Law, Vol. 51, 2015, p. 100.

[15] *Ivi*, p. 83.

[16] Cfr. *Monsanto Co. v. Geertson Seed Farms*, 130 S. Ct. 2743, 2752 (2010); *Horne v. Flores*, 557 U.S. 433, 445 (2009)

[17] Sudha Setty, *op.cit.*, p. 75; cfr. *Al Haramain Islamic Foundation v Obama*, No. 07- 0109 (N.D. Cal. 31/03/2010).

[18] *United States v. U.S. Dist. Court for the Eastern District of Michigan*, 407 U.S. 297, 320 (1997). In questa decisione la Corte Suprema ritenne necessario un mandato da parte del Governo per le attività di sorveglianza elettronica con riferimento a "domestic issues". Tuttavia i parametri stabiliti dalla Corte per la violazione del Quarto Emendamento si riferivano soltanto al concetto di sicurezza interna, restando invece escluso dalla loro applicazione l'ambito delle "foreign intelligence operations".

[19] *Clapper v. Amnesty Int'l* USA, 133 S. Ct. 1138 (2013).

[20] *ACLU v. Clapper*, 959 F. Supp. 2d, 724 (S.D.N.Y. D 27/12/2013).

[21] Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, Pepperdine Law Review, Vol. 42, 2015, p. 773, 815.

[22] *Smith v. Maryland*, 442 U.S. 743-744 (1979).

[23] Cfr. *United States v. Jones,* 132 S. Ct. 945 (2012).

[24] *Katz v. United States*, 389 U.S., p. 360-61.

[25] Per una riflessione sul punto cfr. Megan Blass, *The New Data Marketplace: Protecting Personal Data, Electronic Communications, and Individual Privacy in the Age of Mass Surveillance Through a Return to a Property-Based Approach to the Fourth Amendment*, Hastings Const. L.Q. , Vol.42, 2015, p. 577, 583, 586.

[26] Erin E. Connare, *op. cit.*, p. 395

[27] Cfr. sul punto Caspar Bowden, *The US surveillance programmes and their impact on EU's citizens fundamental rights*, Study for the LIBE Committee, European Parliament, Bruxelles, 2013, p. 16 - 20; Jonathan D. Forgang, *"The*

Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas, Fordham Law Review, Vol. 78, 2009.

[28] *Ivi*, p. 408.

[29] *Amnesty Int'l*, 133 S. Ct., p. 1148.

[30] *ACLU v. Clapper*, 959 F. Supp. 2d 755.

[31] Così anche *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990).

[32] *United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990).

[33] 18 U.S.C. *§* 2712 (a).

[34] *Amnesty Int'l*, 133 S. Ct., p. 1147.

[35] Cfr. *Block v. Chimty Nutrition Inst.*, 467 U.S. 349 (1984).

[36] *ACLU v. Clapper*, V. 14 - 42, Document 168-1, 1503586 (2d Cir. 05/07/2015).

[37] Ciò avvenne in seguito alla sentenza *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

[38] Erin E. Connare, *op.cit.*, p. 406.

[39] Cfr. sul punto Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, Stanford Law Review, Vol. 62, 2010, p. 1005; Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, Fordham Law Review, Vol. 74, 2006, p. 1731.

[40] *ACLU v. Clapper*, V. 14 - 42, Document 168-1, 1503586 (2d Cir. 05/07/2015), p. 90.

[41] H.R. 2048 — 114th Congress (2015-2016), Public Law No: 114-23 (06/02/2015). Disponibile in: https://www.congress.gov/bill/114th-congress/house-bill/2048/text. Accesso effettuato in data 8/7/2015.

[42] Per una disamina specifica della legislazione americana in tema di electronic surveillance cfr. Francesca Bignami, *The US legal system of data*

protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Study for the LIBE Committee, European Parliament, Bruxelles, 2015, p. 21-29; Didier Bigo e altri, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, Study for the LIBE Committee, European Parliament, Bruxelles, 2013p. 25; Caspar Bowden, *op.cit.*, p. 16.

[43] Così *Katz v. United States*, 389 U.S. 360; *United States v. Jones*, 132 S. Ct. 945, 950 (2012). Sul punto cfr. Andrew William Bagley, *Don't be evil: The Fourth Amendment in the Age of Google, National Security, Digital Papers and Effects*, Alb. L.J. Sci. & Tech., 2011, p. 153.

[44] Sudha Setty, *op. cit.*, p. 69.

[45] *Klayman v. Obama*, 957 F. Supp. 2d 1 (D.D.C. 2013).

[46] Margaret Hu, o*p. cit.,* p. 773, 785.

[47] Cfr. Sophie Stalla - Bourdillon - Joshua Phillips Mark D. Ryan, *Privacy v. Security*, Springer, Berlin - Heidelberg, p. 65, 70, 72; Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, Boston College Law Review, Vol. 48, 2007, p. 609; Ira S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, International Data Privacy Law, 2013, p.1.

[48] Corte di Giustizia Europea, Grande Sezione, 8 aprile 2014, Cause riunite C-293/12 e C-594/12. Sul punto cfr. Arianna Vedaschi – Valerio Lubello, *Data Retention and its Implications for the Fundamental Right to Privacy*, Tilburg Law Review, Vol. 20, 2015, p. 14, 18, 26.

[49] Caspar Bowden, *op.cit.*, p. 23.

[50] *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data* (General Data Protection Regulation). Disponibile in: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:52012PC0011&from=EN. Accesso effettuato in data 8/7/2015.

[51] High Court of Ireland, *Maximilian Schrems v. Data Protection Commissioner*, n.765 JR/2013.

[52] Application n. 58170 (04/09/2013).

[53] Francesca Bignami, *Cooperative Legalism and the Non-Americanizaion of Regulatory Styles: The Case of Data Privacy*, The American Journal of Comparative Law, Vol. 59, 2011, p. 412.

[54] Cfr. sul punto James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, Yale L.J. . vol. 113, 2004, p. 1151; William L. Prosser, *Privacy*, California Law Review, Vol. 48, 1960, p. 383; Samuel D. Warren – Louis D. Brandeis, *Right to Privacy*, Harward Law Review, Vol.4, 1890, p. 193.

[55] Cfr. Dennis F. Thompson, *Democratic Secrecy*, Political Science Quarterly, Vol. 114, 1999, p. 181; Maure Goldschmidt, *Publicity, Privacy, and Secrecy*, The Western Political Quarterly, Vol.7, 1954, p. 401; Deirdre Curtin, *Judging EU Secrecy*, Amsterdam Centre for European Law and Governance Working Paper n.7, 2012, p. 12.

[56] Sul punto è interessante, ad esempio, il saggio Cedric Ryngaert, *Clarifying the Extraterritorial Application of the European Convention on Human Rights*, Merkourios, Vol. 28, 2012, pp. 57-60.

[57] Sui tentativi di estensione del Privacy Act Judicial Redress ai cittadini europei cfr. Francesca Bignami, *The US legal system of data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens*, Study for the LIBE Committee, European Parliament, Bruxelles, 2015, p. 13.

Costituzionalismo.it

Fondatore e Direttore dal 2003 al 2014 Gianni **FERRARA**

Email: info@costituzionalismo.it

Registrazione presso il Tribunale di Roma

ISSN: 2036-6744 | Costituzionalismo.it (Roma)