AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

Sicurezza vs protezione dei dati: la CGUE cambia registro

di Michela Tresca *

SOMMARIO: 1. Introduzione. – 2. Primi segnali di cambiamento: la sentenza *Data retention*. – 3. Fine dell'Approdo sicuro: la sentenza *Schrems*. – 4. Conclusioni.

1. Introduzione

L'evoluzione tecnologica e lo sviluppo di Internet hanno posto il diritto alla protezione dei dati personali di fronte a nuove sfide. Le opportunità offerte dalle nuove tecnologie dell'informazione e della comunicazioni, in termini di raccolta e sfruttamento dei dati, hanno reso, infatti, assai più complesso il bilanciamento tra esigenze di protezione e libera circolazione dei dati e delle informazioni personali. Di fronte alle opportunità offerte dallo sviluppo tecnologico, il quadro normativo ha mostrato tutte le sue carenze, e ciò è divenuto ancora più evidente nel momento in cui, con l'entrata in vigore del Trattato di Lisbona[1], il diritto alla protezione dei dati personali è stato elevato a diritto fondamentale dell'Unione. Ci si è trovati, così, a fare i conti non solo con una direttiva[2] evidentemente (totalmente) inadeguata rispetto a un contesto rinnovato, ma anche con un quadro europeo estremamente frammentato, vista l'eterogenea modalità di adattamento da parte di ciascuno Stato membro.

L'inadeguatezza del quadro normativo si è avvertita ancor più di fronte al carattere globale di Internet e al continuo e incessante trasferimento di dati che domina la società attuale. Soprattutto in merito a quest'ultimo aspetto non può essere sottovalutato il quadro internazionale che si è delineato dopo l'11 settembre del 2001. Il rapporto tra sicurezza nazionale e privacy, apparso da sempre come conflittuale, ha finito per risolversi, di fronte alle minacce del terrorismo

* Collaboratrice stabile di @Lawlab - Laboratorio sul Diritto del Digitale, Luiss Guido Carli.

[1] Solo con il Trattato di Lisbona il diritto alla protezione dei dati personali, fino a quel momento semplice parametro di *soft law* trova piena e autonoma costituzionalizzazione: si riconosce alla Carta di Nizza medesimo valore giuridico dei Trattati (art. 6 TUE), Carta che aveva per la prima volta riconosciuto autonoma tutela al diritto alla protezione dei dati personali (art. 8); ancora l'art. 16 TFUE estende il diritto alla protezione dei dati personali a tutte le materie di competenza dell'Unione e l'art. 39 TUE con riguardo alle materie del secondo pilastro (politica estera e sicurezza comune); sul tema cfr. B. CORTESE, *La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona,* in *Dir. Un. eur.,* 2013, pp. 313-336.

[2] Si fa riferimento alla Direttiva 95/46/CE, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,* fino ad oggi testo madre in materia di protezioni dati personali nell'Ue.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

internazionale, enormemente sbilanciato a favore della sicurezza nazionale. La risposta del Governo Usa agli attacchi terroristici è stata l'adozione del *PatriotAct*[3] nel 2001, che ha ridefinito il quadro giuridico dei diritti dei cittadini, ponendo priorità alla sicurezza nazionale rispetto a qualsiasi altro diritto fondamentale, primo fra tutti il diritto alla privacy. Attraverso tale intervento normativo, sono di fatto aumentati a dismisura i poteri di intervento delle agenzie di intelligence e le possibilità, da parte di quest'ultime, di sfruttare il potenziale offerto dai dati. I rischi che potevano essere paventati in virtù di un quadro normativo così delineato sono venuti alla luce con lo scandalo *Datagate*[4].

Le rivelazioni di Edward Snowden hanno mostrato all'opinione pubblica mondiale la gigantesca macchina della sorveglianza posta in essere dal Governo Usa in nome della lotta al terrorismo e della sicurezza nazionale. Un sistema gestito dalle sue principali agenzie di sicurezza, in cui non hanno mancato di rivestire un ruolo di primo piano anche governi europei - la Gran Bretagna al primo posto con la Gchq - e in cui si sono trovati implicati anche i giganti del web, gli stessi che negli ultimi tempi sembrano ergersi a paladini della privacy dei propri utenti[5].

Di fronte al contesto appena delineato, la giurisprudenza ha dovuto svolgere un ruolo non semplice quando chiamata a contemperare il diritto alla protezione dei dati personali con altri diritti e interessi in gioco. Con le pronunce più recenti[6], la CGUE sembra aver intrapreso una strada precisa, che può essere ravvisata nella volontà di affermare con decisione il quadro europeo in materia di protezione dei dati personali. Al riguardo, nell'ultimo biennio si sono susseguite tre sentenze che hanno finito per rafforzare, proprio perché non isolate, il riconoscimento della centralità di tale diritto. Questo è ancor più vero dal momento che oggetto di

[3] Il *Patriot Act*, proprio per rispondere alle minacce alla sicurezza nazionale poste dal terrorismo, ha ridefinito in senso restrittivo i diritti e le libertà dei cittadini; elemento chiave, soprattutto per quel che interessa in questa sede, è l'ampliamento delle intercettazioni delle linee telefoniche e informatiche, attraverso un aumento dei poteri degli organi di polizia e delle autorità federali; tra le previsioni, la sezione 215 ha apportato modifiche al *Foreign Intelligence Surveillance Act* del 1978, permettendo l'accesso alle informazioni detenute dagli ISP, una volta ottenuta l'approvazione giudiziaria.

[4] Lo scandalo *Datagate* è nato in seguito alle rivelazioni di Edward Snowden, pubblicate per la prima volta il 5 giugno 2013 da parte del giornale britannico *The Guardian*; è innanzitutto venuta alla luce la raccolta di metadati da parte dell'*NSA* sulle telefonate dei clienti dell'operatore Verizon; a queste è seguita tutta una serie di rivelazioni circa un vero e proprio sistema di controllo e monitoraggio gestito dall'*NSA*, in collaborazione con le più importanti compagnie telefoniche e operatori Internet; v. A. DI CORINTO- L. REITANO, *Digito ergo spio, le armi del mestiere,* in *Limes,* luglio 2014; F. PIZZETTI, *Datagate, Prism, caso Snowden: il mondo tra nuova grande guerra cibernetica e controllo globale,* in *www.federalismi.it,* 26 giugno 2013.

[5] È nota la vicenda che dal 15 febbraio scorso ha visto instaurarsi un vero e proprio braccio di ferro tra FBI e Apple, in seguito al rifiuto dell'amministratore delegato dell'azienda, Tim Cook, di obbedire all'ordine di un giudice californiano che aveva richiesto la fornitura del software per sbloccare l'i-phone di uno degli attentatori della strage di San Bernardino. La disputa sembra essersi, almeno temporaneamente, risolta a seguito delle rivelazioni dell'FBI sul fatto di essere riuscita ad accedere comunque ai dati del telefono.

[6] Si fa riferimento alla sentenza *Digital Rights Ireland*, Corte di giustizia dell'Unione europea (Grande Sezione), 8 aprile 2014, causa C-293/12; alla sentenza *Google Spain*, Corte di giustizia dell'Unione europea (Grande Sezione), 13 maggio 2014, causa C-131/12 e alla sentenza *Schrems*, Corte di giustizia dell'Unione europea (Grande Sezione), 6 ottobre 2015, causa C-362/14.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

contemperamento con il diritto alla protezione dei dati personali sono diritti ed interessi diversi e segnatamente la pubblica sicurezza, l'iniziativa economica, la libertà d'informazione e di espressione, così come diverse sono le parti coinvolte, trattandosi di rapporti tra persone fisiche e giuridiche, nonché tra cittadini e autorità pubbliche.

Il quadro europeo in materia di protezione dei dati personali è stato così, negli ultimi anni, al centro di un processo di revisione, in cui si sono scontrate due dinamiche, se non opposte, fortemente in conflitto tra loro. Per un verso, si è assistito a una sempre maggiore protezione accordata al diritto alla protezione dei dati personali, anche e soprattutto alla luce delle opportunità e dei rischi introdotti con lo sviluppo tecnologico e ancor più in risposta allo scandalo *Datagate*. Dall'altro lato, soprattutto alla luce delle continue minacce del terrorismo internazionale, si è assistito all'incremento delle garanzie poste a presidio della sicurezza nazionale. Questa seconda dinamica si è concretizzata nella riapertura del dibattito sui *Passenger Name Record (PNR),* sul sistema *SWIFT* o ancora sul sistema *Approdo sicuro*. A questo si aggiunge il fatto che, a livello dei singoli Stati membri, si è registrata una tendenza del legislatore nazionale verso normative restrittive delle libertà a favore di una maggiore sicurezza nazionale[7].

2. Primi segnali di cambiamento: la sentenza *Data retention*

Ad aprire la strada al processo di *enforcement* del diritto alla protezione dei dati personali nell'Ue è la sentenza *Digital Rights Ireland* dell'8 aprile 2014, causa C-293/12. Con tale pronuncia la Corte ha dichiarato invalida la direttiva 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, perché contrastante con il principio di proporzionalità. L'importanza della sentenza è da rinvenire negli effetti della sua pronuncia[8]: innanzitutto con essa la Corte pone fine a quella che si era delineata

[7] Cfr. N. MUIZNIEKS, *Europe in spying on you,* in *www.nytimes.com,* 27 ottobre 2015; S. RODOTÀ nell'intervista riportata da A. ROSSANO, *"Con la scusa del terrorismo ci tolgono i diritti". Stefano Rodotà denuncia la deriva europea,* in *www.espresso.repubblica.it,* 12 maggio 2015; si può citare la legge adottata in Francia il 24 giugno 2015 ("*Loi sur le renseignement"),* con la quale si è ampliato il controllo sulle comunicazioni dei cittadini; tra le previsioni, sussiste un obbligo in capo ai fornitori di telecomunicazioni e ai provider di predisporre "scatole nere" per registrare i metadati delle comunicazioni e delle attività online; alla base di questo controllo, la legge non pone solo ragioni di lotta al terrorismo internazionale, ma anche la salvaguardia della difesa nazionale, interessi superiori di politica estera e di ogni forma di ingerenza straniera, la protezione di importanti interessi economici, industriali e scientifici della Francia, la lotta alla criminalità organizzata e alla proliferazione di armi di distruzione di massa; anche in Italia si è aperto un dibattito molto forte, nel corso dell'approvazione del d.l. antiterrorismo (d.l. n. 7 del 18 febbraio 2015, convertiti in l. n. 43 del 17 aprile 2015), dal cui testo finale è stata eliminata la norma tanto dibattuta che prevedeva la possibilità, per la polizia, di entrare nei computer da remoto per intercettare le comunicazioni via Internet.

[8] Su questo M. NINO, *L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia Ue: prospettive ed evoluzioni future del sistema europeo di data retention,* in *Diritto dell'Unione europea,* 2014, p. 809.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

come una *blanket data retention,* vale a dire un sistema di conservazione di massa di dati, diffuso e generalizzato; sollecita poi l'UE a ripensare il sistema di *data retention* da effettuarsi tenendo presente i diritti fondamentali sanciti dalla Carta dei diritti fondamentali dell'Ue, primi fra tutti il diritto alla riservatezza e il diritto alla protezione dei dati personali. Inoltre, non può essere sottovalutato l'approccio dimostrato dal giudice europeo. In questo senso, si è trattato della prima volta in cui la Corte ha dichiarato invalida una direttiva nella sua interezza, a cui si aggiunge il fatto che tale invalidità è stata disposta *ex tunc* ed in ragione della non conformità alla Carta dei diritti fondamentali[9].

La pronuncia deriva da due controversie originate rispettivamente in Irlanda e in Austria[10]; in entrambi i casi il giudice nazionale aveva mosso rinvio pregiudiziale di fronte alla Corte di Giustizia per verificare la validità della normativa sulla *data retention.* La Corte imposterà la sua argomentazione seguendo un filo che può essere riassunto in tre tappe, attraverso le quali si propone, come prima cosa, di verificare la rilevanza degli articoli 7 e 8 della Carta di Nizza per valutare la validità della direttiva; in secondo luogo, va a verificare se la stessa costituisca ingerenza nei diritti di cui ai medesimi articoli e, infine, se tale ingerenza possa ritenersi giustificata[11].

Per quanto riguarda la prima questione, la Corte rileva come l'art. 3 della direttiva, imponendo per i fornitori un obbligo generalizzato di conservazione dei dati, chiama in causa tanto il diritto al rispetto della vita privata e familiare (art.7), quanto il diritto alla protezione dei dati personali (art.8), a nulla rilevando che la Direttiva espressamente escluda dal suo ambito di applicazione il contenuto della comunicazione. Si potrebbe infatti ugualmente delineare, a opinione della Corte, un'influenza sulla libertà di espressione degli utenti, sostanziandosi inoltre un'invasione nella sfera privata e una compromissione della protezione dei dati personali. L'ingerenza della Direttiva negli articoli 7 e 8 della Carta viene quindi qualificata come «di vasta portata» e «particolarmente grave»[12]. Constatata

[9] La severità dimostrata dalla Corte evidenzierebbe la sua considerazione circa la gravità della violazione di diritti fondamentali posta in essere dall'atto invalidato. Sul punto, cfr. S. CRESPI, *Diritti fondamentali, Corte di giustizia e riforma del sistema Ue di protezione dei dati,* in *Rivista italiana di diritto pubblico comunitario*, 2015, p.834, la quale evidenzia come, in questo modo, i giudici Ue hanno sollecitato la Commissione e il legislatore europeo a ripensare la struttura generale dell'atto.

[10] Si tratta delle cause C-293/12 e C-594/12, le quali, essendo simili quanto a contenuto della domanda, saranno decise dalla CGUE con la sentenza in cause riunite l'8 aprile 2014; nel primo caso si trattava di un ricorso da parte della Digital Rights Ireland di fronte alla Corte irlandese, con il quale si contestava la validità della Direttiva 2006/24 e la parte settima della legge del 2005 sulla giustizia penale nel porre un obbligo di conservazione dei dati di traffico; la Corte sospende il giudizio e muove rinvio pregiudiziale di fronte alla CGUE, chiedendo in particolare la conformità di alcune disposizione della direttiva con il principio di proporzionalità, nonché di valutare la compatibilità con il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali; nel secondo caso, il Verfassungsgerichtshof era stato investito da una serie di ricorsi con i quali si chiedeva l'annullamento dell'art. 102 bis della legge sulle telecomunicazioni, considerato in violazione del diritto alla protezione dei dati personali; anche in questo caso, viene sospeso il giudizio per sottoporre alla CGUE la valutazione della conformità della direttiva alla luce del diritto alla vita privata, il diritto alla protezione dei dati e la libertà di espressione.

[11] In questo senso M. NINO, *cit.*, p. 807.

[12] Punto 37 della Sentenza.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

l'ingerenza, la Corte passa poi a valutare se essa possa risultare giustificata alla luce dell'art. 52 della Carta, il quale prescrive che limitazioni dei diritti e delle libertà in essa garantiti trovano giustificazione qualora siano previsti
dalla legge e ne venga rispettato il contenuto essenziale, rispettino il principio di proporzionalità o siano necessari a perseguire gli scopi di interesse generale. È alla luce di questi tre profili che la Corte procede nella sua valutazione circa la legittimità dell'ingerenza constatata. Se i primi due profili passano il vaglio della Corte, nel momento in cui la verifica si sposta al punto centrale della valutazione, vale a dire la proporzionalità dell'ingerenza constatata, le conclusioni portano ad un esito negativo. Ad essere contestata è innanzitutto la generalità delle disposizioni, che comporterebbero un controllo rivolto all'intera popolazione europea, a prescindere dalla sussistenza o meno di sospetti circa quella determinata persona e della sussistenza di rischi, anche solo in ipotesi, per la sicurezza pubblica, cosa che facilmente potrebbe condurre a un sistema di sorveglianza di massa.

Ad essere rilevata, inoltre, è la mancanza di un criterio oggettivo nei confronti dell'azione di accesso ai dati da parte delle autorità nazionali competenti e che non porterebbe a limitare le persone autorizzate ad accedere ed utilizzare tali dati, così come la mancanza della previsione di un controllo preventivo da parte di un giudice o di un'entità amministrativa indipendente sull'accesso ai dati conservati. Genericità e mancanza di specificità si rileva anche per quel che concerne la durata della conservazione. La Direttiva mancherebbe, infine, nel garantire la sicurezza e la protezione dei dati, anche alla luce del fatto che non si pone alcun obbligo di conservare i dati sul territorio dell'Unione.

È alla luce di questi motivi che la Corte invalida la Direttiva 2006/24/CE. Può essere rilevato a questo punto come, se il legislatore europeo nel giungere a delineare uno strumento normativo come quello della direttiva del 2006 era stato condizionato dal clima creatosi all'indomani degli attentati terroristici di Londra e Madrid, altrettanto il giudice europeo, nel provvedere a invalidare lo stesso strumento, è stato con buone probabilità influenzato dalle rivelazioni di Snowden e dall'emersione di un vero e proprio sistema di sorveglianza di massa[13]. La Corte, infatti, verrà a ritenere che nessuna esigenza di sicurezza nazionale, e nel caso di specie neanche la minaccia terroristica, può giustificare un'ingerenza così generalizzata e indeterminata nei riguardi del diritto fondamentale alla protezione dei dati personali. L'eco del *Datagate* può essere rintracciato soprattutto nel punto in cui la Corte sottolinea l'esigenza che i dati oggetto di conservazione per ragioni di giustizia restino nel territorio dell'Ue.

È chiaro, a questo punto, che la sentenza ha aperto degli scenari importanti e in particolare, se ha posto degli interrogativi nel breve periodo, non manca di delinearne altri in un'ottica di più lungo periodo. Un primo interrogativo riguarda la validità delle normative nazionali in materia di *data retention*, molte delle quali di diretto recepimento della direttiva invalidata. Se alcuni Stati membri già prima della pronuncia della Corte si erano mossi nel senso di invalidare le rispettive

[13] In questo senso O. PREVOSTI, *Tutela della privacy come presupposto della libertà: due recenti sentenze della Corte di Giustizia dell'Unione Europea a difesa della riservatezza individuale,* in *www.osservatorioaic.it*, settembre 2014, p. 2.

normative nazionali in materia[14], e altri lo hanno fatto subito a seguito dell'intervento del giudice di Lussemburgo[15], ci sono paesi in cui esse permangono in vigore.

Tra questi, l'Italia ha recepito la direttiva 2006/24/CE con il d.lgs 109/2008 e con alcune modifiche al Codice della privacy, in particolare all'art. 132[16]. Tale quadro normativo non è stato ancora intaccato dalla pronuncia della Corte di Giustizia, sebbene non siano mancati interventi che, all'indomani della pronuncia, hanno rilevato la non compatibilità dell'art. 132 con il quadro normativo europeo[17].

La pronuncia della Corte, però, non si limita a riversare i suoi effetti sul piano interno, nei confronti degli Stati membri, ma ha inevitabili ricadute anche a livello internazionale. Ad essere chiamati in causa potrebbero essere, ad esempio, gli accordi USA-UE sui *PNR*[18], vale a dire sulla raccolta dei dati dei passeggeri aerei, anch'essi conclusi all'interno della lotta al terrorismo e dunque guardando a finalità di sicurezza nazionale[19]; lo stesso potrebbe dirsi per il sistema *SWIFT*[20] riguardante il trasferimento di dati bancari dei cittadini europei al governo americano.

Alla luce di quanto riportato, occorre capire se quanto disposto dalla Corte nella sentenza in esame debba essere limitato alla direttiva invalidata o se abbia un inevitabile riflesso anche su ambiti ad essa vicini e che, come quelli appena esposti, vedono comunque al centro la conservazione e il trasferimento di dati alla luce della sicurezza nazionale e della lotta al terrorismo e alla criminalità.
Risulta chiaro, a questo punto, come l'intervento della Corte abbia mantenuto - se non contribuito a delineare - un quadro poco chiaro e incerto, che richiederebbe

[14] V. Corte suprema amministrativa bulgara, decisione n. 13627 dell'11 settembre 2008; Corte costituzionale rumena, decisione n.2158 dell'8 ottobre 2009; Corte costituzionale federale tedesca del 2 marzo 2010; Corte costituzionale ceca del 22 marzo 2011; Corte suprema cipriota del 1 febbraio 2011; sul punto v. T. KONSTADINIDES, *Destroying Democracy on the Ground of Defending It? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem,* in *European law review*, 2011, pp. 722-736.
[15] Si tratta di Regno Unito, Svezia, Danimarca e Olanda.
[16] L'art. 132 del d.lgs. 196/2003 al I comma prevede, per finalità e accertamento dei reati, la conservazione, da parte del fornitore, per 24 mesi dei dati telefonici e per 12 mesi dei dati telematici, sempre con esclusione del contenuto delle comunicazioni.
[17] In tal senso F. IOVENE, *Data retention tra passato e futuro. Ma quale presente?,* in *Cassazione penale,* 2014, p. 4276-4267, la quale rileva che, alla luce dei parametri definiti dalla Corte, non risultando tale disposizione conforme al diritto primario dell'Unione, sarebbe necessaria la disapplicazione, nel caso concreto, da parte del giudice interno eventualmente investito della questione.
[18] GUUE L 215 dell'11 agosto 2012.
[19] Su questo S. CRESPI, *cit*., pp. 840-841, si chiede, a fronte di quanto statuito dalla CGUE, come potrebbe considerarsi conforme l'accordo PNR che dispone, tra le altre cose, il trasferimento dei dati a prescindere dai sospetti circa un soggetto e quindi di fatto un controllo di massa; o ancora nel momento in cui si apre la possibilità di utilizzare i PNR anche per reati minori, o non si prevede un coinvolgimento delle autorità garanti indipendenti degli Stati membri o ancora, sul profilo della conservazione di tali dati, dispone un periodo di cinque anni come dati personalizzati e altri dieci spersonalizzati e comunque non prevedendo, superati i quindici anni, una loro cancellazione, quanto piuttosto solo l'anonimizzazione.
[20] GUUE L 195 del 27 luglio 2010.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

un intervento da parte delle istituzioni europee, alle quali tra l'altro sono rivolte linee guida[21] per l'introduzione di un nuovo sistema di *data retention* all'interno della garanzia dei diritti fondamentali. In questo senso, in un'ottica di lungo periodo, un ruolo centrale in materia dovrebbe quindi essere svolto dalle istituzioni europee, non mancando di coinvolgere anche le istituzioni internazionali e i rapporti di quest'ultime con le prime.

3. Fine dell'approdo sicuro: la sentenza *Schrems*

La sentenza del 6 ottobre 2015, causa C-362/14, ribadisce ancora una volta e con una maggiore eco oltreoceano, l'attenzione dimostrata di recente dalla CGUE nei confronti del diritto alla protezione dei dati personali.

Com'è noto, il caso ha origine dalla richiesta rivolta dallo studente austriaco Max Schrems alla filiale irlandese di Facebook di avere accesso ai dati che lo riguardavano a disposizione del *social network*. Dopo un iniziale rifiuto dell'azienda, Schrems aveva successivamente ricevuto oltre milleduecento pagine raggruppanti tutti i suoi dati di cui Facebook disponeva dal momento della sua iscrizione, avvenuta nel 2008, tra cui risultavano anche dati dallo stesso cancellati. Decide, così, di presentare ventidue ricorsi all'autorità garante irlandese (*Data Protection Commisioner*) lamentando - anche alla luce di quanto rilevato da Edward Snowden sulle attività condotte dalla NSA all'interno del programma PRISM[22] e i legami con le maggiori aziende operanti in Internet - la mancanza di una protezione dei dati personali una volta trasferiti in Usa. Ad essere messi in discussione sono dunque, di fatto, i trasferimenti di dati personali da Facebook Irlanda a Facebook Usa di fronte a un accesso generalizzato che le autorità statunitensi avrebbero su questi dati.

Il *Commissioner*, pur stilando un rapporto contenente alcune indicazioni rivolte a Facebook, respinge la denuncia di Schrems, rinvenendo, alla luce della decisione di adeguatezza della Commissione Europea[23] sul *Safe Harbor*[24], non solo la

[21] In questo senso M. MESSINA, *La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati n*ell'ambito della fornitura di serv*izi* di comunicazione elettronica e *ne dichiara la loro invalidità,* in *Ordine internazionale e diritti umani*, 2014, pp.396-401, il quale evidenzia, tra le linee guida deducibili dalla sentenza, la proporzionalità all'obiettivo da perseguire come base di legittimità di qualsiasi attività di conservazione dei dati personali, il superamento dello schema previsto dalla direttiva 2006/24 e in particolare il sistema di raccolta generalizzato che essa aveva posto in essere; infine la considerazione dell'aspetto della trasferibilità dei dati.

[22] PRISM è il programma di sorveglianza elettronica di massima segretezza, posto in essere dalla *National Security Agency* (*NSA*, Agenzia di intelligence statunitense) a partire dal 2007, per raccogliere dati di traffico Internet e telefonico mondiale con lo scopo iniziale della lotta al terrorismo e in base al quale il governo statunitense ha potuto richiedere alle Big di Internet di avere accesso alle mail, ai video, alle chat e a qualsiasi altra informazione dell'utente, avendo come base di legittimità il *Foreign Intelligence Surveillance Act*.

[23] Commissione Europea, Decisione 2000/520/CE, (Gazzetta ufficiale n. L 215 del 25/8/2000), la quale ha riconosciuto validità ai *Safe Harbor Privacy Principles*, il rispetto dei quali costituisce base per riconoscere l'adeguatezza del trattamento di dati da parte di imprese statunitensi.

[24] Il *Safe Harbor* è un accordo Usa-Ue del 2000, con il quale le aziende americane si impegnano volontariamente a rispettare i principi generali previsti dalla normativa Ue in materia di protezione

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

garanzia di un «livello adeguato di protezione dei dati a carattere personale», ma anche l'assenza di una sua competenza nel giudicare l'adeguatezza di tale sistema, alla luce della primazia del diritto comunitario su quello interno. Impugnata la decisione di fronte all'Alta Corte d'Irlanda, quest'ultima sottopone una questione pregiudiziale davanti alla Corte di Giustizia. Nello specifico, il giudice di merito chiede alla Corte di Lussemburgo se l'autorità irlandese fosse vincolata dalla Decisione della Commissione, come d'altronde dall'autorità stessa sostenuto, o se potesse, o meglio dovesse, procedere autonomamente con un'inchiesta per valutare l'adeguatezza offerta dal sistema Usa ai dati in esso trasferiti a fronte di doglianze di un cittadino europeo.

Con la pronuncia in esame, e segnatamente rispondendo al quesito pregiudiziale sottopostogli, la Corte arriva a valorizzare il ruolo delle autorità garanti nazionali di protezione dei dati. Guardando all'art. 28[25] della Direttiva letto alla luce dell'art. 8 della Carta dei diritti fondamentali dell'Unione, riconosce in capo alle autorità nazionali di garanzia il potere di giudicare conforme a quanto prescritto dagli artt. 25 e 26 della direttiva stessa[26] il trasferimento di dati verso paesi terzi. In particolare, viene sottolineato come, nell'azione tesa a garantire la protezione dei dati personali, le autorità di controllo devono procedere a un bilanciamento tra l'osservanza del diritto alla privacy e il libero scambio di dati personali. Tale potere viene riconosciuto anche in casi, come quello di specie, dove sussiste una decisione della Commissione circa l'adeguatezza del trasferimento.

In questo senso, pur rilevando la prevalenza della Commissione nel procedere a tale valutazione di adeguatezza e la preclusione per le autorità nazionali di adottare decisioni contrarie a quanto già statuito dall'esecutivo europeo, non ritiene che questo possa precludere la possibilità, per l'interessato, di richiedere all'autorità garante nazionale di valutare l'adeguatezza del trasferimento dei dati nello Stato terzo[27]. Tuttavia, la Corte riconosce solo in capo ad essa il potere di invalidare o meno una decisione della Commissione.

Da quanto statuito dalla Corte, le autorità nazionali non possono, quindi, respingere la richiesta di verifica di adeguatezza del sistema loro pervenuta da

---

dei dati personali, qualora si trovino a trattare dati di cittadini Ue; alcuni principi alla base di tale accordo riproducono infatti quelli statuiti dalla Direttiva 95/46/CE.

[25] L'art. 28, prevedendo per ciascuno Stato membro la predisposizione di almeno un'autorità di controllo, fornisce un elenco esemplificativo dei poteri da riconoscere in capo ad esse e in particolare poteri investigativi, poteri d'intervento - tra cui formulare pareri, disporre la cancellazione, la distruzione dei dati - ed infine il potere di promuovere azioni giudiziarie.

[26] L'art. 25 dispone, in linea generale, il divieto di trasferimento dei dati al di fuori del territorio dell'Unione, a meno che lo Stato terzo non garantisce un "livello di protezione adeguato" e al di là delle deroghe poste a tale divieto nell'articolo successivo - consenso dell'interessato, il trasferimento sia necessario per la conclusione o esecuzione di un contratto, salvaguardia dell'interesse pubblico o dell'interesse vitale dell'interessato, sussistenza di un registro pubblico che permette un accesso ai dati oggetto del trasferimento; sempre l'art. 25 riconosce poi in capo alla Commissione europea il compito di valutare tale adeguatezza.

[27] Tale conclusione, tra l'altro, trova riscontro in quanto statuito dal paragrafo 4 dell'art. 28 della Direttiva 95/46/CE, che dispone: «Qualsiasi persona, o associazione che la rappresenti, può presentare a un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento dei dati personali. […]».

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

parte di un cittadino europeo che nutra, nel caso di specie, dei dubbi sul grado di tutela accordato ai suoi dati. In definitiva, la High Court irlandese, ad avviso della Corte, avrebbe dovuto rispondere alle richieste ad essa rivolte dal sig. Schrems e verificare essa stessa la legittimità del trasferimento dei dati personali verso gli Stati Uniti.

Nonostante il chiaro e perentorio iter argomentativo seguito dalla Corte, rimangono, tuttavia, alcune incertezze sull'effettivo ruolo riconosciuto alle autorità garanti[28]. Innanzitutto, la Corte non specifica se sussista in capo a queste ultime la possibilità di adottare provvedimenti volti a sospendere o vietare i trasferimenti di dati. Questo è ancor più vero dal momento che la decisione della Commissione del 2000, anche se limitatamente a condizioni specifiche, riconosceva in capo alle autorità stesse il potere di sospendere il trasferimento dei dati verso un'organizzazione che aveva sottoscritto i principi di approdo sicuro in conformità con le FAQ[29].

Al di là dei profili connessi al ruolo dei garanti nazionali - che risulta indubbiamente assai rafforzato dal giudice europeo, nella direzione di valorizzare e rafforzare la tutela apprestata all'individuo - la Corte di Lussemburgo va ben oltre la domanda pregiudiziale e invalida nella sua interezza la decisione della Commissione 2000/520/CE. Sotto questo secondo profilo, la Corte arriva, non solo, ad intaccare e mettere in dubbio il sistema di trasferimento di dati che ormai aveva trovato nella decisione la sua base di legittimità, ma colpisce alle fondamenta l'intero sistema di trattamento di dati da parte dei grandi colossi del web[30]. A rappresentare il punto centrale sul quale si muovono le valutazioni della Corte, comunque, non è tanto la tutela accordata ai dati personali dai singoli operatori dei *social media*, e nello specifico la legittimità delle politiche di trattamento operate da Facebook, ma il sistema di sorveglianza di massa posto in essere dagli Usa in particolare dopo gli attacchi dell'11 settembre e nel quale i grandi gestori dei servizi Internet si sono trovati implicati; la valutazione del giudice europeo ha riguardato, quindi, più che altro la compatibilità di tutto tale sistema con il quadro europeo di protezione dei dati personali[31].

Ovviamente, ad essere stati messi in discussione sono i rapporti tra Usa e Ue in materia, e ad essere chiamati in causa non sono solo gli Over the top e segnatamente Facebook, sulla cui attività muovono i dubbi del ricorrente nella causa principale, ma le circa 4500 imprese che hanno sede negli Stati Uniti e che legittimamente hanno sottoscritto tale regime, così come sulle imprese che

[28] S. CRESPI, *cit.,* p. 14.

[29] Art. 3, par. 1, Decisione 2000/520/CE, il quale dispone che la sospensione del trasferimento da parte delle autorità nazionali possa avvenire nel caso in cui «abbiano accertato che l'organizzazione viola i principi applicati in conformità alle FAQ» oppure nel caso in cui «sia molto probabile che i principi vengano violati», «vi siano ragionevoli motivi per ritenere che l'organismo di esecuzione competente non stia adottando o non adotterà misure adeguate e tempestive per risolvere un caso concreto».

[30] In questo senso P. FALLETTA, *La Corte di Giustizia, ancora una volta, contro le multinazionali del web (riflessioni su Corte di Giustizia UE (Grande sezione), 6 ottobre 2015, Schrems c. Data Protection Commissioner, C-362/14),* in *www.federalismi.it,* 23 dicembre 2015, p. 3.

[31] Cfr. B. SAETTA, *Il 6 ottobre l'Europa processa Facebook e lo spionaggio americano?,* in *www.valigiablu.it,* 5 ottobre 2015.

dall'Europa trasferiscono dati in Usa. Gli effetti della sentenza, già a questo punto chiaramente estesi, finiscono poi per riverberarsi anche sugli Stati terzi che hanno sottoscritto accordi con l'Ue in materia di trasferimento dei dati[32], potendo impattare anche su Stati terzi che hanno preso l'Ue solo come modello per l'adozione dei rispettivi accordi[33].

Ora, se si legge la sentenza come un'ulteriore presa di posizione della Corte a favore del diritto alla privacy, può essere accolto con favore il percorso particolarmente rigoroso che è stata ormai intrapreso dal giudice europeo[34]. Al riguardo, sono stati numerosi i giudizi positivi, se non entusiastici, sul rinnovato determinismo della Corte di Giustizia rispetto alle fonti comunitarie, specie nell'affermazione della primazia riconosciuta ai diritti della persona, primo fra tutti il diritto alla protezione dei dati personali. In questo senso, i giudici europei sono considerati i principali attori che riaffermano la prevalenza dei diritti dell'individuo sugli interessi economici, di fronte a scelte di politica legislativa che sembrano andare nel senso opposto[35]. Nella stessa direzione, si può citare il favore con il quale il Garante nazionale ha accolto la pronuncia della Corte, a cui va il merito di rimettere «al centro dell'agenda degli Stati il tema dei diritti fondamentali delle persone e la necessità che questi diritti, primo fra tutti la protezione dei dati, vengano tutelati anche al di fuori dei confini europei»[36].

Non manca chi ha evidenziato anche alcune debolezze alla base della pronuncia[37]. Primo fra tutti, il fatto che la Corte sia andata al di là di quanto strettamente richiesto dal giudice del rinvio ed abbia quindi ampliato la sua discrezionalità fino a pronunciarsi sulla validità dell'atto. Inoltre, sembra mancare di riscontro pratico la lamentata assenza di verifica da parte della Commissione circa la sussistenza di misure di tutela, che sembrano, al contrario, essere presenti all'interno del sistema *Safe Harbor* e specificamente nelle FAQ. Infine, per quanto concerne il rischio paventato sulla violazione del diritto alla protezione dei dati personali, soprattutto alla luce di deroghe previste all'applicazione delle sue previsioni, può essere rilevato che prescrizioni analoghe a quelle che si rinvengono nella decisione sono presenti anche nella direttiva 95/46/CE[38].

---

[32] Gli Stati che fino ad oggi hanno ottenuto la decisione di adeguatezza da parte della Commissione per il trasferimento dei dati dall'Ue: Andorra, Argentina, Canada, Isole Faeroe, Guernsey, Israele. Isola di Man, Jersey, Nuova Zelanda, Svizzera, Uruguay.

[33] È il caso, ad esempio, della Svizzera che aveva concluso con gli Usa lo *US- Swiss Safe Harbor* seguendo il modello adottato dall'Ue e la cui autorità garante, in seguito alla pronuncia della CGUE ha sospeso la legittimità dell'accordo fino alla negoziazione del nuovo; su questo, cfr. S. CRESPI, *cit*..

[34] La sentenza è stata accolta in questo senso con favore da gran parte della dottrina; cfr. S. RODOTÀ, *Internet e privacy, c'è un giudice in Europa che frena gli Usa*, *www.repubblica.it*, 12 ottobre 2015, e M. BASSANINI- O. POLLICINO, *La Corte di giustizia demolisce il safe harbor e ridisegna i confini del diritto alla privacy in ambito transnazionale,* in *www.diritto24.il sole24ore.com*, 7 ottobre 2015.

[35] S. RODOTÀ, *ult. cit*..

[36] Facebook: dichiarazione di Antonello Soro sulla sentenza della Corte di giustizia Europea, 6 ottobre 2015, disponibile su www.garanteprivacy.it

[37] P. FALLETTA, *cit*., p. 7.

[38] *Ibidem*.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

A questo punto, viene naturale chiedersi la ragione per cui una pronuncia di invalidità sia giunta a quindici anni di distanza dall'entrata in vigore di un sistema che ha continuato fino ad oggi a regolare i trasferimenti di dati verso gli Usa e che, nonostante rilievi critici già evidenziati in passato[39], era stato mantenuto invariato. Non possono essere sottovalutati, a questo riguardo, gli effetti prodotti dallo scandalo *Datagate* e quanto da esso rivelato, che ha indubbiamente gettato un occhio di discredito nei confronti di qualsiasi soggetto operante oltreoceano, potenziale collaboratore della gigantesca macchina della sorveglianza.

Ancora da considerare sono le due pronunce della Corte *Google Spain* e la già illustrata *Digital Rights Ireland*, che segnano la strada intrapresa dal giudice europeo nel sancire la primazia del diritto alla privacy sul trattamento dei dati effettuato dai gestori di servizi Internet. In linea con le due pronunce del 2014, l'ultimo intervento della Corte, non solo sembra sferrare un attacco alle multinazionali del web, ma si pone nel senso di voler anticipare quanto il legislatore europeo non è riuscito per lungo tempo a portare a termine, disegnando una giurisprudenza che sembra svolgere un ruolo ancillare, se non sostitutivo, rispetto alla politica.

4. Conclusioni

Alla luce delle pronunce più recenti, è chiaro il ruolo rivestito dalla Corte di Giustizia in materia di protezione dei dati personali, in un contesto nel quale la politica è parsa rincorrere principi che hanno per lungo tempo trovato tutela solo a livello giurisdizionale. Non può essere sottovalutata, in questo senso, l'accelerazione imposta al legislatore da parte del giudice europeo.

In primo luogo, il processo di riforma dell'intero quadro europeo in materia di protezione dei dati personali, iniziato nel 2012 su proposta della Commissione europea[40], ha solo a distanza di quattro anni – e precisamente il 14 aprile scorso -

[39] È interessante notare come la stessa Commissione, a quattro anni dall'approvazione della decisione, aveva evidenziato alcuni interventi migliorativi da apportare; v. Documento di lavoro dei servizi della Commissione sull'attuazione della decisione 520/2000/CE della Commissione sull'adeguatezza offerta dai principi di approdo sicuro e dalle relative "domande più frequenti" (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (SEC (2004) 1323), 20 ottobre 2004; più di recente, sempre la Commissione è intervenuta con due interventi richiamati anche nella sentenza - Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, (COM(2013) 846 final,), 27 novembre 2013 e Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «approdo sicuro» dal punto di vista dei cittadini dell'UE e delle società ivi stabilite (COM(2013) 847 final,), 27 novembre 2013 - ; in tale contesto, tra l'altro, non è mancato un intervento diretto del Parlamento europeo a favore della sospensione degli accordi *Safe Harbor*, Relazione sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni (2013/21888(INI).

[40] Si fa riferimento al pacchetto di riforma che si compone di una Comunicazione della Commissione europea, *Salvaguardare la privacy in un mondo interconnesso. Un quadro europeo della protezione dei dati per il XXI secolo,* COM(2012) 9 final; una Proposta di regolamento del Parlamento e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento*

visto la sua conclusione con l'approvazione definitiva da parte del Parlamento europeo del Regolamento sulla protezione dei dati, che da qui a due anni andrà a sostituire la Direttiva 95/46/CE e le rispettive normative nazionali di recepimento. Su questo, non può essere sottovalutato il ruolo anticipatorio delle pronunce della CGUE su ambiti che trovano oggi tutela nel nuovo testo[41], e che hanno animato per lungo tempo il dibattito politico, motivo quest'ultimo del ritardo nella definizione del nuovo quadro.

In secondo luogo, soprattutto con la Sentenza *Schrems*, si è imposta un'accelerazione ai negoziati tra Usa e Ue in materia di trasferimento dei dati. Deve essere tenuto conto che negoziati su un nuovo accordo erano stati aperti già da due anni, anche alla luce delle nuove condizioni in cui si erano trovati ad operare i principi del *Safe Harbor* rispetto al momento della loro stipula. Dopo l'entrata in vigore della Decisione è stato infatti approvato il *Partiot Act* che, tra le altre previsioni, ha riconosciuto maggiori poteri di intrusione da parte delle agenzie federali a fronte della lotta al terrorismo. Tutte le potenziali ingerenze che potevano immaginarsi sono poi venite alla luce con lo scandalo *Datagate*. Le esigenze di maggiore tutela, palesatesi di fronte al nuovo quadro, si sono però scontrate con un'*impasse* nel procedere a nuovi negoziati. Dopo l'invalidazione della decisione della Commissione sull'adeguatezza del regime *Approdo sicuro*, non sono di fatto stati dichiarati illegittimi o vietati i trasferimenti di dati verso gli Usa, ma si è senza dubbio delineato un quadro di profonda incertezza in materia, circostanza che ha fatto avvertire più che mai l'esigenza di giungere ad un nuovo accordo.

Il 2 febbraio 2016, al di là del termine fissato[42], è stato raggiunto un primo accordo politico sul punto e il 29 febbraio è stata data la notizia della presentazione dei testi giuridici dell'Usa-UE *Privacy Shield* da parte della Commissione europea[43]. Questo accordo, subentrando al vecchio *Safe Harbor*, rappresenterà il nuovo quadro sullo scambio commerciale dei dati al di là dell'Atlantico. Sarebbe interessante ora capire l'opinione della CGUE sul nuovo quadro che verrà a imporre obblighi più precisi per le società che si trovano a trattare dati, con una maggiore vigilanza del loro operato e sanzioni o esclusione in caso di inadempienza; per la prima volta gli Stati Uniti hanno fornito una garanzia scritta all'Ue, affinché qualsiasi azione da parte delle autorità pubbliche

---

dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati), COM(2012)11 e infine una proposta di Direttiva del Parlamento europeo e del Consiglio *concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di protezione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati,* COM(2012)10.

[41] Si pensi, tra gli altri, al diritto all'oblio, all'ambito di applicazione territoriale della normativa europea, al trasferimento dei dati personali.

[42] In seguito alla pronuncia della CGUE, il Gruppo Art. 29 aveva emesso un Comunicato con il quale, nel definire la necessità di una stretta applicazione della sentenza, fissava al 31 gennaio il termine per trovare un nuovo accordo Usa-Ue sul trasferimento dei dati, pena la possibilità per le autorità di protezione nazionali di poter prendere tutte le misure necessarie; di fatto, dunque, era stata sospesa qualsiasi azione da parte dei garanti nazionali, salvando momentaneamente il trasferimento di dati al di là dell'Atlantico.

[43] Il testo della *Draft adequacy decision* è disponibile sul sito della Commissione al seguente indirizzo: http://europa.eu/rapid/press-release_IP-16-433_it.htm.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

al fine della sicurezza nazionale sia sottoposta a precisi limiti, controlli e che sia impedito qualsiasi accesso generalizzato ai dati dei cittadini Ue; proprio con riferimento a questi ultimi, il nuovo quadro intende accordare loro una maggiore protezione, prevedendo in particolare in capo ad essi adeguate possibilità di ricorso, tra le quali quella di rivolgersi a un Ombudsperson in relazione al trattamento dei loro dati da parte delle forze dell'ordine e delle agenzie di Intelligence statunitensi; infine, è stato previsto un meccanismo annuale di revisione congiunto degli accordi da parte della Commissione europea e del Ministero del Commercio degli Stati Uniti.

Sulla *Draft adequasy decision* presentata dalla Commissione il 13 aprile, si è già pronunciato, tra l'altro, il Gruppo art. 29[44], il quale ha criticato il nuovo accordo che continuerebbe a non garantire una reale protezione dei cittadini europei nei confronti della sorveglianza posta in essere dagli Usa[45]. Pur mostrando apprezzamento per i miglioramenti che il *Privacy Shield* introduce rispetto al quadro che fino ad oggi ha regolato il trasferimento dei dati oltreoceano - in particolare in riferimento ad una maggiore trasparenza e all'accesso ai dati nel quadro della sicurezza nazionale - il *Working Party* non ha mancato di evidenziare alcuni elementi di criticità. In particolare, è stata ravvisata la necessità di rendere conforme tali previsioni al nuovo quadro europeo in materia di protezione dei dati personali, introdotto con il Regolamento. Per quanto riguarda l'utilizzo dei dati da parte delle autorità pubbliche al fine di tutelare la sicurezza nazionale, il Gruppo art. 29 rinviene una mancata garanzia contro eventuali raccolte massicce e indiscriminate di dati. Tre sono, nello specifico, i punti indicati dal Gruppo art. 29 come ancora critici e sui quali ha formulato le sue raccomandazioni e auspica un intervento della Commissione europea; innanzitutto il tenore delle disposizioni non obbligherebbe le organizzazioni a cancellare i dati una volta venuta meno la necessità della loro conservazione; dall'*Annex VI* della *Draft adequacy decision* si evincerebbe, in secondo luogo, che l'amministrazione statunitense non esclude completamente la possibilità di far ricorso a una raccolta massiva e indiscriminata di dati; infine, con riferimento all'Ombudsperson, mancherebbero chiare e precise previsioni quanto ai poteri di indipendenza e all'effettiva operatività di tale figura[46].

Il parere del Gruppo dei Garanti non è certo vincolante, ma potrà avere degli effetti sui termini dell'accordo, soprattutto alla luce della possibilità, per i Garanti nazionali - come tra l'altro da ultimo riconosciuto dalla CGUE nella sentenza *Schrems* - di indagare sui trasferimenti di dati dei cittadini europei e di poter agire

[44] Il Gruppo art. 29, istituito dall'art.29 della Direttiva 95/46/CE, è un organismo consultivo indipendente composto da un rappresentante delle autorità nazionali di protezione dei dati personali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione europea.

[45] WP238, *Opinion 01/2016 on the EU- U.S. Privacy Schield draft adequacy decision,* 13 April 2016.

[46] È bene tener presente che, nelle valutazioni portata avanti dal Gruppo art. 29, si è tenuto conto di quattro garanzie essenziali: 1) il trattamento dei dati deve essere basato su "*regole chiare, precise e accessibili*"; 2) l'accesso ai dati dei cittadini europei deve essere limitato ai principi di "necessità e proporzionalità"; 3) l'esistenza di un "meccanismo di controllo indipendente, efficace e imparziale"; 4) la garanzia di "rimedi efficaci" per i cittadini europei.

AMMINISTRAZIONE IN CAMMINO
Rivista elettronica di diritto pubblico, di diritto dell'economia e di scienza dell'amministrazione a cura del Centro di ricerca sulle amministrazioni pubbliche "Vittorio Bachelet"
Direttore Professor Giuseppe Di Gaspare
ISSN 2038-3711

in giudizio, nel caso riscontrassero una violazione dei diritti fondamentali, a prescindere dalla sussistenza di qualsiasi accordo. Spetta ora all'esecutivo europeo prendere di nuovo in mano l'accordo e a quel punto si vedrà se e in quali termini esso si configurerà nei prossimi mesi.