Schrems colpisce ancora? Il trasferimento dei dati personali dall'Unione europea a Stati terzi, le Conclusioni dell'Avvocato generale nel caso *Data Protection Commissioner v. Facebook Ireland Limited e Maximillian Schrems* e una storia che rischia di ripetersi

Giulia Formici

Sommario

Keywords

trasferimento di dati personali - Schrems - *Standard Contractual Clauses* - decisione di adeguatezza - protezione dei dati personali

1. Il cd. caso *Schrems* II tra passato e presente (ovvero del complesso intreccio tra storiche pronunce e rinvii pregiudiziali pendenti dinnanzi alla Corte di giustizia dell'Unione europea)

In un mondo sempre più globalizzato e digitalizzato, il quotidiano e ormai indispensabile trasferimento, dall'Unione europea a Stati terzi, di dati e metadati digitali, da parte di soggetti privati, ha fatto sorgere questioni e problematiche giuridiche di grande rilievo, non ancora del tutto risolte e ancora oggi oggetto di forte dibattito. L' "esportazione" di dati al di fuori dei confini europei, infatti, si traduce quasi sempre in un passaggio dagli elevati standard di protezione della riservatezza garantiti dall'apparato normativo europeo e degli Stati membri, a livelli di tutela inferiori predisposti dagli

ordinamenti degli Stati riceventi[1]. L'esigenza dunque di conciliare il flusso di dati personali con la garanzia dei diritti fondamentali protetti agli artt. 7 e 8 della Carta di Nizza, ha portato l'UE a predisporre, prima nella direttiva 95/46/CE e, successivamente, nel GDPR[2], un insieme di disposizioni volte ad autorizzare il trasferimento solo nel caso in cui nello Stato terzo venga garantito un "adeguato" livello di protezione dei dati. A tale scopo, la Commissione può emanare una decisione attestante l'adeguatezza delle tutele predisposte dalla legislazione o dagli impegni internazionali del Paese ricevente ed avente valenza generale per tutti i trasferimenti verso di esso, mentre, in mancanza di tale decisione, il flusso di dati può essere consentito mediante il ricorso a strumenti alternativi quali l'inserimento di c.d. *Standard Contractual Clauses* (SCCs) all'interno dei contratti tra esportatori ed importatori di dati. Proprio relativamente a quest'ultimo meccanismo ed, in particolare, alla validità della decisione 2010/87/UE della Commissione[3] che fissa un elenco di clausole contrattuali tipo utilizzabili, la Corte di giustizia dell'UE è stata chiamata a pronunciarsi nel caso *Data Protection Commissioner v. Facebook Ireland e Maximillian Schrems* (C-311/18). Mentre la decisione di questa controversia è attesa con trepidazione dagli attivisti per la privacy e tiene col fiato sospeso i giganti del mondo digitale, grande interesse e contrastanti reazioni hanno suscitato le Conclusioni dell'Avvocato generale Saugmandsgaard Øe, depositate il 19 dicembre 2019 e che si vogliono in questa sede annotare. Prima di analizzarne il contenuto ed elaborare alcune riflessioni conclusive, pare però necessario ricostruire, pur brevemente, le vicende giudiziarie che hanno condotto sino alla Corte di giustizia, prendendo abbrivio dalla prima storica pronuncia *Schrems*[4]: se infatti il primo capitolo della "saga" che vede contrapposto il giovane cittadino austriaco Maximillian Schrems al gigante blu dei social network ben può essere definito come un terremoto con epicentro nell'Oceano Atlantico, tra continente europeo e Stati Uniti, il caso oggetto di questo contributo ne è il conseguente tsunami, che rischia di abbattersi con forza sulle coste americane[5].
In estrema sintesi e rinviando alla ampia letteratura in materia[6], nel 2013 Schrems si

[1] Sul punto si legga Commissione Europea, *Scambio e protezione dei dati personali in un mondo globalizzato*, COM (2017) 7 final, 10 gennaio 2017.

[2] Il GDPR ha ampliato le scarne disposizioni dedicate al trasferimento dei dati verso Stati terzi indicate nel Capo IV della direttiva 95/46/CE, riservandovi ben 8 articoli del Capo V e 19 Considerando. Per ulteriori approfondimenti su questa articolata disciplina, si rinvia, tra i tanti a M. Leffi, *I trasferimenti di dati verso Stati terzi nel nuovo Regolamento UE*, in *Rivista di Diritti Comparati*, 2, 2017, 187 ss.

[3] Modificata poi con decisione della Commissione 2016/2297 del 16 dicembre 2016.

[4] CGUE, C-362/14, *Maximillian Schrems v. Data Protection Commissioner* (2015).

[5] Merita solo accennare come, tra la prima pronuncia del 2015 e il caso ad oggi pendente, lo stesso Schrems abbia azionato una ulteriore causa dinnanzi ai giudici austriaci, giunta anch'essa alla Corte di giustizia ed avente quale controparte sempre il Golia dei Social Network, Facebook (C-498/16, *Maximilian Schrems v. Facebook Ireland Limited*). Questa pronuncia tuttavia ha lasciato sullo sfondo le questioni direttamente attinenti alla tutela dei dati e della riservatezza, per concentrarsi su problematiche riguardanti l'attribuzione dello status di consumatore ad un utente di social network e l'applicabilità dell'art. 16, Reg. 44/2001.

[6] *Ex multis*, S. Carrera-G. Elspeth, *The end of Safe Harbour: what future for EU-US data transfers?*, in *Maastricht Journal of European and Comparative Law*, 3, 2015, 1 ss.; M. Nino, *Le prospettive internazionali ed europee della tutela della privacy e dei dati personali dopo la decisione Schrems della CGUE*, in *Diritto dell'informazione e dell'informatica*, 4, 2015, 577 ss.; X. Tracol, *'Invalidator' strikes back: the harbour has never been safe*, in *Computer Law and Security Review*, 3, 2016, 345 ss.; G. Resta-V. Zeno Zencovich (a cura di), *La protezione transnazionale*

rivolgeva, senza successo, al *Irish Data Protection Commissioner* (DPC) per ottenere una pronuncia di sospensione del trasferimento dei propri dati personali dalla controllata Facebook Ireland a Facebook Inc. con sede negli USA. Tale richiesta era motivata dalla convinzione che, contrariamente da quanto accertato dalla Commissione nella sua decisione 2000/520/CE sulla base del regime di cd. "approdo sicuro" e alla luce delle rivelazioni di Edward Snowden circa l'esistenza di programmi di *mass surveillance* – in particolare Upstream e Prism – posti in essere dalla National Security Agency americana (NSA), il livello di protezione dei dati negli USA non potesse essere considerato sufficiente a garantire una adeguata tutela della vita privata da intromissioni generalizzate e indiscriminate. Dinnanzi al respingimento del proprio ricorso, Schrems impugnava il provvedimento del DPC dinnanzi alla High Court irlandese la quale riteneva necessario l'intervento della Corte di giustizia: quest'ultima, con una pronuncia dalla storica portata, dichiarava l'invalidità della decisione di adeguatezza sopra richiamata. I principi volti a garantire la protezione dei dati e della riservatezza, indicati nell'accordo "approdo sicuro", risultavano infatti applicabili solo a soggetti privati e non anche alle autorità pubbliche: queste ultime potevano dunque conservare, accedere e trattare i dati provenienti dall'UE senza dover sottostare a tali limiti, ingerendo così nei diritti fondamentali tutelati dagli artt. 7 e 8 della Carta di Nizza in maniera sproporzionata e non limitata a quanto strettamente necessario, senza peraltro assicurare un adeguato accesso a rimedi giurisdizionali[7].

All'indomani della sentenza *Schrems*, le imprese stanziate nell'UE si trovavano in una situazione di forte incertezza operativa, dovendo adottare ed implementare, in maniera rapida ed efficace, meccanismi alternativi necessari al legittimo trasferimento Oltreoceano dei dati personali di utenti europei, in assenza di una decisione di adeguatezza. La necessità di individuare una chiara via d'uscita da tale *empasse* risultava prioritaria sia per le autorità statunitensi quanto per l'UE, nella consapevolezza, sopra evidenziata, che un blocco o una maggiore rigidità e difficoltà di circolazione dei dati, nell' "economia dell'informazione" attuale, si sarebbe tradotta in ingenti perdite e in un dannoso isolamento dell'Unione dal mercato globale. Questa situazione critica ed instabile spiega come in – relativamente – poco tempo e mediante colloqui intensificati, si sia addivenuti ad un nuovo regime di trasferimento dati, il *Privacy Shield*, che è stato poi posto alla base della successiva e attualmente vigente decisione di adeguatezza della Commissione per il flusso di dati UE-USA (2016/1250)[8].

In tale articolato contesto, la controversia che aveva dato origine al rinvio pregiudiziale del caso *Schrems* tornava nelle mani del giudice del rinvio: la High Court irlandese, an-

dei dati personali. Dai 'Safe Harbour Principles' al 'Privacy Shield', Roma, 2016; S. Crespi, *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *DPCE*, 3, 2016, 687 ss.

[7] Oltre a fornire una prima specificazione del termine, estremamente vago, di "adeguatezza", definendolo come "sostanziale equivalenza" del livello di protezione garantito dello Stato terzo rispetto a quello tutelato nell'UE, la Corte di giustizia stabiliva come non possa essere considerata limitata allo stretto necessario una normativa che autorizza la conservazione generalizzata dei tutti i dati personali di tutte le persone i cui sono trasferiti negli USA e come sia lesiva del contenuto essenziale del diritto al rispetto della vita privata una normativa che consenta un accesso generalizzato alle autorità pubbliche del contenuto di telecomunicazioni.

[8] COM (2016) 1250, 12 luglio 2016, sull'adeguatezza della protezione offerta in ragione dello Scudo UE-USA per la privacy.

nullando la previa decisione del DPC avverso il ricorso di Schrems, rinviava a tale autorità il caso per una nuova decisione che tenesse conto dei rilievi della Corte di giustizia. L'originaria doglianza dell'attivista austriaco però necessitava di essere riformulata, indicando una nuova base giuridica del trasferimento dati Oltreoceano: non potendo più fondarsi sull'ormai invalidata decisione 2000/520/CE, Schrems individuava la fonte del flusso di dati tra la sede irlandese e quella americana di Facebook nell'accordo c.d. *Data transfer processing Agreement*, concluso tra le due aziende nel 2015 ed integrante le SSCs indicate dalla Commissione nella richiamata decisione 2010/87; il ricorrente sosteneva che tali clausole non fossero idonee a garantire alcun diritto di accesso alla giustizia negli USA e che, ancora una volta, il livello di protezione dei dati e della riservatezza offerto, anche dalle clausole contrattuali tipo, non potesse considerarsi sostanzialmente equivalente a quello europeo. La rinnovata richiesta di sospensione del trasferimento dati dunque portava il DPC ad aprire una articolata inchiesta, conclusasi con l'avvio di un procedimento dinnanzi alla High Court affinché questa provvedesse a predisporre un ulteriore rinvio pregiudiziale alla Corte di giustizia, ritenendo necessaria, ai fini della risoluzione del caso, una pronuncia circa la validità della decisione della Commissione in materia di SCCs. L'analisi dei giudici irlandesi è estremamente articolata, come dimostrato non solo dagli 11 quesiti posti ai giudici di Lussemburgo ma anche dalle ben 152 pagine della pronuncia, comprensiva di un Annex contenente studi circa la normativa americana, le tutele da essa predisposte e il funzionamento dei sistemi di sorveglianza[9]. Le ampie questioni del rinvio riguardano dunque, riassuntivamente, l'applicabilità del diritto europeo e delle tutele da esso sancite anche nel caso in cui i dati trasferiti vengano trattati nello Stato terzo per scopi di sicurezza nazionale; la conformità alla Carta di Nizza e al diritto europeo delle garanzie offerte dalle SCCs e dunque la validità stessa della decisione della Commissione 2010/87; il rapporto tra tale decisione e quella di adeguatezza, basata sul regime *Privacy Shield* nonché, indirettamente, la validità di quest'ultima.

Come risulta chiaro da questa, pur succinta, ricostruzione delle vicende giudiziarie nonché dei numerosi quesiti posti all'attenzione della Corte di giustizia nel rinvio pregiudiziale in esame, sono ancora molti gli interrogativi aperti e gli aspetti incerti relativi alla disciplina del trasferimento di dati personali verso Stati terzi ed, in particolare, verso gli USA. La delicatezza della attesissima pronuncia dei giudici di Lussemburgo risiede non solo nell'importanza e complessità delle questioni poste, nel loro potenziale impatto economico nonché nel campo delle relazioni internazionali e nella determinazione, come si dirà meglio anche nelle conclusioni, della posizione dell'UE nel dibattito globale circa la tutela della riservatezza e della protezione dei dati ma anche, nella dimensione interna all'Unione stessa: si fa riferimento cioè agli effetti che tale decisione potrà avere sui numerosi rinvii pregiudiziali pendenti in materia di trasferimento di

[9] *The Data Protection Commissioner v. Facebbok Ireland Limited e Maximillian Schrems,* 4 maggio 2018, n. 4809, 2016. Per una analisi del contenuto della pronuncia della High Court irlandese, si rinvia a R. Cabazzi, *Irish High Court e Corte di giustizia europea: un nuovo dialogo sul trasferimento di dati da Facebook Ireland a Facebook Inc.*, in *questa Rivista,* 1, 2018, 473 ss. Si noti che Facebook Ireland Limited ha impugnato la decisione della High Court dinnanzi alla Corte Suprema irlandese, che ha respinto tali istanze con sentenza del 31 maggio 2019, *The Data Protection Commissioner v. Facebook Ireland Limited and Maximillian Schrems*, Appeal no. 2018/68.

dati e di *data retention* per scopi securitari. Come ben mette in luce l'Avvocato generale nelle sue Conclusioni e come si vuole preliminarmente sottolineare, il caso in analisi si intreccia inscindibilmente sia con il ricorso di annullamento, promosso da *La Quadrature du Net* insieme ad altre associazioni francesi, avverso la decisione di adeguatezza in materia di trasferimento dati UE-USA più volte richiamata[10], sia con i casi *Privacy International*, *La Quadrature du Net* e *Ordre des Barreaux Francophones*[11], anch'essi fortemente attesi e osservati con grande attenzione soprattutto dai governi nazionali ed aventi ad oggetto la disciplina della conservazione e accesso ai metadati per scopi securitari. Tali rinvii pongono infatti questioni rilevanti sul piano della determinazione dell'ambito di applicazione del diritto dell'UE e dei principi emersi dalla sua giurisprudenza anche con riferimento ad attività che attengono alla sfera della sicurezza nazionale – area di esclusiva pertinenza degli Stati membri[12]. A questo scenario fatto di rimandi e di riflessi continui con casi pendenti, è da aggiungersi un ulteriore profilo di complessità, derivante dalla connessione delle questioni in esame con la giurisprudenza della Corte europea dei diritti dell'uomo: come si dirà nel prossimo paragrafo, le pronunce ed i principi in materia di tutela della privacy dinnanzi a pratiche di raccolta, conservazione e accesso massivi (c.d. *bulk interception*), delineati dai giudici di Strasburgo, sono stati infatti individuati dall'Avvocato generale come criterio di raffronto per determinare la "sostanziale equivalenza" del livello di protezione garantito dallo Stato terzo laddove non risulti applicabile il diritto dell'UE. Il riferimento a tale copiosa ed articolata giurisprudenza è reso ancor più difficile dai quesiti ad oggi ancora aperti dinnanzi alla Corte europea dei diritti dell'uomo stessa, come dimostrato dai fondamentali e rilevanti casi *Big Brother Watch* e *Centrum for Rattvisa* in materia di *mass surveillance* al momento oggetto di ricorso innanzi alla Grande Camera[13].

La complessità delle questioni da affrontare, unitamente alle molteplici connessioni con altri casi pendenti di cruciale importanza sia sul fronte esterno del trasferimento dei dati che su quello interno della *data retention*, rendono dunque il panorama europeo estremamente intricato: le lunghe e tutt'altro che semplici Conclusioni dell'Avvocato generale nel caso in esame ne sono il riflesso

[10] T-738/16, *La Quadrature du Net e altri v. Commissione,* promossa il 25 ottobre 2016. Non a caso l'udienza di questo caso, fissata agli inizi di luglio del 2019, è stata poi sospesa dalla Corte di giustizia per concentrarsi prima sulla risoluzione del rinvio qui in esame e ad esso connesso.

[11] C-623/17, *Privacy International v. Secretary of State for Foreign and Commonwealth Affairs e altri*; cause riunite C-511/18 e C-512/18, *La Quadrature du Net e altri v. Premier Ministre e altri*; C-520/18, *Ordre des Barreaux Francophones e altri v. Conseil des Ministres*. Si segnala che il 15 gennaio 2020 sono state consegnate le Conclusioni dell'Avvocato generale in tutti questi tre interessanti quanto fondamentali casi, dagli attesi effetti dirompenti per quanto attiene gli strumenti a disposizione di autorità di *law enforcement* e servizi di intelligence e la proporzionalità e stretta necessità degli stessi.

[12] Per una ricostruzione dei citati rinvii pregiudiziali e del loro potenziale impatto, si veda: D. Fennelly, *Data retention: the life, death and afterlife of a Directive*, ERA Forum, pubblicato online il 25 giugno 2018; E. Celeste, *The Court of Justice and the ban on bulk data retention: expansive potential and future scenarios*, in *European Constitutional Law Review*, 1, 2019, 134 ss.; sia concesso anche il richiamo a G. Formici, *Tutela della riservatezza delle comunicazioni elettroniche: riflessioni (ri)partendo dalla pronuncia Ministerio Fiscal*, in *Osservatorio costituzionale AIC*, 3, 2018, 453 ss.

[13] CEDU, *Centrum For Rattvisa v. Svezia*, ric. 35252/08 (2018) e *Big Brother Watch e altri v. Regno Unito*, ricc. 58170/13, 62322/14 e 24960/15 (2018), attualmente entrambi al vaglio della Grande Camera, dal febbraio 2019.

2. Le conclusioni dell'Avvocato generale: dalle *Standard Contractual Clauses* al *Privacy Shield*

Come anticipato, i quesiti posti dal giudice irlandese nel rinvio pregiudiziale hanno ad oggetto svariati aspetti e sfaccettature della disciplina del trasferimento dei dati. Volendosi concentrare, in questa sede, sulle questioni di maggior rilievo e sulle più importanti posizioni espresse dall'Avvocato generale, pare utile suddividere le Conclusioni in tre "sezioni": la prima riguardante l'ambito di applicazione del diritto dell'UE nei casi di successivo trattamento per finalità di sicurezza nazionale dei dati trasferiti; la seconda attinente alle SCCs e alla validità della relativa decisione ed infine, la terza, nella quale vengono affrontati gli interrogativi circa la validità della decisione di adeguatezza riguardante il trasferimento dati UE-USA e dal regime di Scudo per la privacy ad essa connesso.

Partendo dunque dalla prima questione, Saugmandsgaard Øe chiarisce sin dall'inizio un punto di estrema importanza: al fine di determinare l'applicabilità del diritto europeo alle operazioni di *data transfer* a scopo commerciale, l'unico elemento da considerare è l'attività all'interno della quale il flusso di dati ha luogo, mentre lo scopo alla base di qualsiasi ulteriore trattamento dei dati trasferiti, anche da parte di pubbliche autorità del Paese di destinazione, risulta del tutto irrilevante (§ 105). Del resto è lo stesso art. 45, c. 2 del GDPR a precisare che, nell'ambito della valutazione di adeguatezza del livello di protezione offerto nello Stato ricevente, la Commissione debba valutare anche le normative straniere inerenti alla tutela della sicurezza nazionale, portando a ritenere dunque che tali previsioni e l'eventuale trattamento dei dati a tale scopo non porti per sé stessa ad una esclusione dell'applicabilità del diritto europeo e non faccia rientrare l'utilizzo dei dati in quelle eccezioni espresse dagli artt. 3, c. 2, della superata direttiva 95/46/CE e 2, c. 2, del vigente GDPR[14]. L'Avvocato generale dunque conclude sul punto ritenendo che il trasferimento dei dati oggetto di esame nel caso sottoposto alla Corte di giustizia faccia indubbiamente parte dello svolgimento di una attività commerciale, essendo così ad esso applicabile il diritto dell'UE e le normative in materia di privacy e *data transfer*, indipendentemente da ogni successivo utilizzo o trattamento, per qualsivoglia finalità.

Spostandoci poi al secondo ordine di quesiti affrontati nelle Conclusioni e dunque addentrandoci nello specifico ambito delle SCCs, viene innanzitutto chiarito il livello di protezione che questi strumenti debbono garantire. Ecco che l'Avvocato generale esprime preliminarmente una valutazione di non poco conto e dalle importanti conseguenze: anche le clausole contrattuali tipo, così come le decisioni di adeguatezza, debbono garantire un livello di protezione dei dati e della riservatezza "sostanzialmente equivalente" a quello europeo; usando le parole di Saugmandsgaard Øe «*the requirements of protection of fundamental rights guaranteed by the Charter do not differ according to the legal basis for a specific transfer*» (§ 117). Quello che invece differisce è la modalità con la quale

[14] Tali disposizioni escludono dal proprio ambito di applicazione il trattamento di dati "effettuato per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione" (art. 2, par. 2, GDPR), quali appunto la protezione della sicurezza nazionale, riservata agli Stati membri dall'art. 4, par. 2, del TUE.

la continuità del livello di tutela viene mantenuta: mentre la decisione di adeguatezza accerta lo standard di protezione garantito in un preciso Stato terzo e, come si è già avuto modo di sottolineare, con valenza generale per tutti i trasferimenti dati verso di esso, nel caso delle SCCs è invece l'"esportatore" di dati che, mediante la predisposizione e il rispetto delle clausole contrattuali, assicura standard di protezione adeguati; la ratio sottostante alla previsione delle clausole tipo come meccanismo alternativo di trasferimento dati è quindi proprio quella di sopperire e compensare alla assenza di una decisione di adeguatezza generale: la decisione 2010/87 della Commissione fissa pertanto le clausole tipo inseribili nei *data transfer agreements* al fine di garantire la sostanziale equivalenza della tutela dei diritti alla riservatezza e protezione dei dati, indipendentemente dal Paese di destinazione e dunque dal livello di protezione da esso garantito. Quest'ultima valutazione dello specifico Stato e delle garanzie offerte dal suo ordinamento diviene però fondamentale in un momento successivo alla previsione delle SCCs nei contratti tra esportatore e importatore di dati: gli obblighi derivanti dall'ordinamento del Paese terzo ricevente, infatti, potrebbero entrare in conflitto con le condizioni stabilite nelle clausole tipo ed impedirne quindi il rispetto da parte del *data importer*. Chiamato a valutare la conformità della decisione 2010/87 ai diritti sanciti nella Carta di Nizza, l'Avvocato generale ritiene, sulla base di tale premessa, che la validità di tale disposizione dipenda dalla sussistenza di meccanismi che permettano una sospensione o un divieto del trasferimento laddove venga accertato che le SCCs non possono essere rispettate nell'ordinamento straniero di destinazione. Il fatto dunque che tali clausole siano vincolanti unicamente per i soggetti sottoscriventi il contratto di trasferimento non ne comporta l'invalidità: l'adeguato livello di protezione dei diritti fondamentali infatti è garantita, secondo l'Avvocato generale, dal fatto che le SCCs previste nella decisione della Commissione, unitamente ai poteri attribuiti alle autorità di controllo nazionali degli Stati membri, individuino in capo a queste ultime e ai *data exporter* (e ai loro responsabili del trattamento) un obbligo di controllo circa la concreta possibilità di attuazione e rispetto delle clausole nel contesto dell'ordinamento dello Stato ricevente e, in caso contrario, il vincolo di provvedere a che il trasferimento non abbia luogo. Viene pertanto attribuito un dovere in capo in primis all'esportatore e, in caso di inerzia di quest'ultimo, alle autorità nazionali di controllo, con un intervento quindi suppletivo, di svolgere verifiche, di grande delicatezza e complessità, per ogni specifico trasferimento dati e dunque caso per caso: una forte responsabilizzazione – anche dei soggetti privati – che, come si vedrà nelle considerazioni conclusive, ha destato perplessità sul fronte della sua concreta realizzabilità. Pur ammettendo di non poter ignorare tali dubbi e preoccupazioni[15], espresse anche dal DPC irlandese, l'Avvocato generale considera la decisione 2010/87 valida sulla base della valutazione dei poteri assegnati dal GDPR (art. 58, par. 2) alle autorità di controllo e dei singoli responsabili del trattamento: insomma l'impossibilità di applicare le garanzie stabilite nel contratto di trasferimento, a causa degli obblighi imposti dall'ordinamento dello Stato ricevente, non implica l'incompatibilità del meccanismo alternativo delle SCCs rispetto

[15] Il DPC irlandese mette anche in luce il rischio che, attribuendo una tale responsabilità alle singole autorità nazionali, si possa venire a creare un panorama frammentario di soluzioni differenti da Stato a Stato. Sul punto l'Avvocato generale ritiene che «*the risk that the approaches taken by the different supervisory authorities will be fragmented is inherent in the decentralised surveillance structure intended by the legislature*» (§ 155).

alla Carta di Nizza poiché ad una potenziale situazione di inadeguatezza delle tutele sopperisce l'obbligo di sospensione o divieto del flusso dei dati (§ 158).
Giunto ad una tale conclusione, Saugmandsgaard Øe non ritiene necessario provvedere all'analisi e soluzione degli ulteriori quesiti promossi dal giudice del rinvio: la pronuncia sulla validità della decisione della Commissione in materia di SCCs, infatti, consente alla High Court irlandese e al DPC di risolvere il ricorso promosso da Schrems, senza il bisogno di valutare anche la decisione di adeguatezza sul trasferimento dati UE-USA e dei connessi principi sanciti nel *Privacy Shield*. Tale questione, sollevata indirettamente dalla Corte irlandese, comunque fosse affrontata, non andrebbe ad incidere sulle considerazioni sino ad ora svolte in materia di clausole contrattuali tipo; sulla base delle osservazioni previamente svolte, una analisi *in concreto* dell'incompatibilità degli obblighi stabiliti dall'ordinamento statunitense con le tutele inserite nelle SCCs è compito precipuo di ogni singolo *data controller* e, in caso di inerzia di questo, delle autorità nazionali di controllo: la Corte di giustizia, ad opinione dell'Avvocato generale, non dovrebbe quindi sostituirsi al DPC irlandese ed imbarcarsi in una valutazione definita "precipitosa" e "prematura". Sebbene non venga negato che la valutazione dei sistemi di sorveglianza posti in essere dalle autorità di intelligence statunitensi sia elemento rilevante per la soluzione del ricorso dell'attivista austriaco che il DPC irlandese sarà chiamato a risolvere, viene tuttavia consigliato alla Corte di giustizia «*not to give a ruling on those questions with the sole aim of helping the DPC to deal with that complaint, when there is no need to answer them in order to allow the referring court to resolve the dispute in the main proceedings (..); in ruling on the problem described above [la validità della decisione di adeguatezza], the Court would to my mind disrupt the normal course of the procedure that will have to take place after it has delivered its judgement in present case*» (§§ 178-180), senza considerare il fatto che una tale valutazione è già oggetto di una azione di annullamento già pendente dinnanzi alla medesima Corte nel caso *La Quadrature du Net*, sopra richiamato[16].
Nonostante questa premessa, Saugmandsgaard Øe reputa comunque necessario sviluppare alcune riflessioni sulla decisione 2016/1250, nel caso in cui i giudici di Lussemburgo decidano di distanziarsi dall'approccio suggerito. Pur precisando sin da subito il carattere non esaustivo delle proprie considerazioni (§ 196), nonché stabilendo che l'esistenza di una decisione di adeguatezza non impedisce alle autorità di controllo nazionali di sospendere o vietare il trasferimento di dati effettuato sulla base delle SCCs, differenziando e distaccando così le due valutazioni (§ 194), l'Avvocato generale svolge una lunga e dettagliata analisi del sistema statunitense e, in particolare, dei programmi di sorveglianza Prism e Upstream, del loro funzionamento e delle fonti normative che li regolano, utilizzando le informazioni fornite, tra gli altri, dal governo statunitense e dalla articolata ricostruzione della High Court irlandese. Anche in questa sezione però sorge preliminarmente una questione connessa all'ambito di applicazione del diritto dell'UE, che condiziona poi tutta la successiva analisi: se infatti l'adeguatezza del livello di protezione assicurata in uno Stato terzo deve essere

[16] L'Avvocato generale suggerisce poi che, nel caso in cui il DPC, anche in sede di riesame del ricorso avanzato da Schrems, reputasse essenziale per la risoluzione della controversia una pronuncia della Corte di giustizia in materia di validità della decisione di adeguatezza riguardante il trasferimento dati UE-USA, allora essa dovrebbe trasferire il caso alla High Court affinché questa, come avvenuto nel caso in esame, predisponga un rinvio ai giudici di Lussemburgo (§. 180).

determinata sulla base di un raffronto e comparazione tra regole e pratiche attuative proprie dello Stato terzo e livello di protezione garantito nell'UE, bisogna chiedersi quale sia innanzitutto il criterio per determinare le attività di trattamento dei dati alle quali è applicabile il diritto europeo, al fine poi di stabilire quale sia il parametro di confronto e dunque i principi da valutare per attestare l'adeguatezza della protezione fornita da un ordinamento straniero. Riprendendo l'interpretazione già fornita nelle proprie conclusioni del caso *Ministerio Fiscal*[17], l'Avvocato generale stabilisce un punto determinante e passibile di avere riflessi anche per gli altri casi pendenti dinnanzi alla Corte di giustizia aventi ad oggetto la dimensione interna della disciplina della *data retention*: il diritto dell'Unione ed i suoi principi non si applica alle attività di trattamento (conservazione, raccolta, accesso) per scopi securitari unicamente poste in essere dallo Stato e da autorità pubbliche, senza il coinvolgimento di soggetti privati; si rientra invece nel campo d'azione del diritto europeo e, dunque, dei principi e requisiti da esso stabiliti anche per mezzo degli interventi giurisprudenziali, nei casi in cui, sempre per scopi di sicurezza nazionale, venga richiesto dalle autorità pubbliche l'intervento e la collaborazione dei providers di servizi di telecomunicazioni: questo alla luce del coinvolgimento di attività di trattamento dei dati da parte di operatori commerciali ed indipendentemente dalla sussistenza o meno di un obbligo in capo agli stessi di conservazione dei dati[18]. Seguendo questo ragionamento, siccome la mera "messa a disposizione" di dati e metadati su richiesta di autorità pubbliche rientra nella definizione di trattamento dei dati e rappresenta dunque una attività svolta dai service providers, una tale attività e le disposizioni che la regolano rientrano conseguentemente nell'ambito di applicazione del diritto europeo e delle normative in materia di tutela della riservatezza e protezione dei dati[19]. Chiarito questo generale principio, con riferimento al sistema statunitense di raccolta, conservazione e trattamento, per scopi securitari, dei dati personali, anche – ma non solo – provenienti dall'UE, l'Avvocato generale opera una distinzione: fanno parte della seconda categoria di attività sopra descritte, implicanti un trattamento svolto anche da soggetti privati, la Section 702 del *Foreign Intelligence Surveillance Act* (FISA). Questa normativa consente, in estrema sintesi, alla NSA di emanare ordini diretti agli operatori dei servizi di telecomunicazione stanziati negli USA di effettuare ricerche tra i dati in loro possesso – mediante appositi *selectors* o *search criteria* – e di mettere le informazioni ottenute a disposizione della autorità statunitensi. Questi ordini vengono preventivamente vagliati e approvati da una apposita corte, la US *Foreign Intelligence Surveillance Court* (FISC), che non è chiamata però a svolgere valutazioni circa l'esistenza di una "*probable cause*" e di sospetti a motivazione della sorveglianza e della raccolta di dati richiesta. Tale tipologia di attività, implicando

[17] CGUE, *Ministerio Fiscal*, C-207/16 (2018).

[18] Questo approccio, accolto dall'Avvocato generale, è ciò che emerge dai casi *Tele2* e *Ministerio Fiscal*, mentre differisce da una previa interpretazione della stessa Corte nella pronuncia *European Parliament v. European Council and Commission* (cause riunite C-317/04 e C-318/04) (2006). Per questo interessante confronto, rilevante anche in materia di *data retention*, sul fronte interno, si rimanda ai §§ 214-225.

[19] «*I conclude that (..) the GDPR and therefore the Charter apply to national rules that require a provider of electronic communications services to lend its assistance to the authorities responsible for national security by making data available to them, where appropriate after having filtered them, even independently of any legal obligation to retain the data*» (§ 223).

l'intervento e il trattamento di dati da parte di service providers, rientrano nell'ambito di applicazione del diritto UE: il livello di adeguatezza delle tutele predisposte rispetto a tali misure deve essere quindi valutato alla luce della Carta di Nizza, del GDPR e dei criteri stabiliti dalla giurisprudenza della Corte di giustizia in materia ed è pertanto nello standard di garanzia previsto dall'Unione che deve essere individuato il parametro di raffronto nella valutazione di adeguatezza. Ebbene, sotto tale profilo l'Avvocato generale rileva come anche la mera messa a disposizione dei dati, nonché le operazioni di filtraggio e la conservazione effettuate dai *data importer* su richiesta delle autorità statunitensi rappresentano intrusioni ed interferenze nel diritto alla privacy e alla protezione dei dati; esse non rappresentano però, diversamente da quanto stabilito nella prima sentenza *Schrems*, una lesione dell'essenza del diritto alla privacy. L'accesso ai dati effettuato dalle agenzie di intelligence, infatti, in tale sistema, non può essere considerato "generalizzato", essendo anzi targettizzato grazie alle previe operazioni di "filtraggio" dei dati sulla base di appositi *search criteria*. Non mancano però di essere rilevate talune criticità nel sistema di sorveglianza statunitense, individuate innanzitutto nella carenza di chiarezza e precisione nel delimitare i confini del ricorso a tali mezzi di invasioni della sfera privata, nonché sotto il profilo della proporzionalità e necessità e della insufficienza delle garanzie esistenti, incapaci di prevenire il rischio di abusi da parte delle autorità pubbliche. Sotto tali profili quindi Saugmandsgaard Øe esprime dubbi quanto alla idoneità delle normative che regolano tali programmi di *surveillance* di assicurare un adeguato livello di tutela ai dati trasferiti.

Nella prima categoria di attività di sorveglianza, quella cioè che comprende operazioni di trattamento dei dati che non implicano un intervento o azione di soggetti privati, bensì unicamente delle autorità pubbliche, rientrano invece gli *Executive Order 12333*. Questi ultimi autorizzano l'NSA ad accedere direttamente ai cavi posti sotto l'Oceano Atlantico e attraverso i quali i dati vengono trasferiti dall'UE agli USA. Tali *orders* non sono sottoposti ad un previo controllo giudiziario e non sono previsti neppure rimedi giurisdizionali successivi attivabili dai soggetti sorvegliati e i cui diritti si ritengono lesi dal trattamento operato. L'unico limite posto a tali misure è quello stabilito dalla *Presidential Policy Directive 28* (PPD 28) introdotta da Obama a seguito delle rivelazioni di Snowden e che è volta a limitare l'uso di tali mezzi di sorveglianza in maniera più limitata possibile e a prevedere in capo ai membri della Intelligence Community l'onere di implementare nuove misure e policies volte a rafforzare la tutela della privacy. Non essendo riconducibili all'ambito di applicazione del diritto europeo, quest'ultimo non può fungere da parametro nella valutazione dell'adeguatezza delle tutele predisposte: l'Avvocato generale quindi individua nella Convenzione europea dei diritti dell'uomo e nella giurisprudenza della Corte sita in Strasburgo il criterio da considerare rispetto a tali operazioni. Sotto questo profilo, l'analisi dell'Avvocato generale si basa su due premesse interessanti: innanzitutto sul il fatto che «*the standards resulting from Articles 7, 8 and 47 of the Charter as interpreted by the Court [CGUE] are in certain respects stricter than those arising under Articole 8 of the ECHR according to the interpretation of those provisions by the ECtHR*» (§ 251) e, secondariamente, che dinnanzi a quest'ultima Corte sono pendenti alcuni rilevanti casi, già evidenziati sopra – *Big Brother Watch* e *Centrum for Rattvisa* - nei quali i giudici di Strasburgo dovranno riconfermare o riconsiderare alcuni

dei principi sanciti nella sua giurisprudenza più recente. Tenendo conto di tali aspetti quindi Saugmandsgaard Øe ritiene che l'*Order* 12333 non sia supportato da idonee tutele – considerate alla luce di quel criterio che la Corte europea dei diritti dell'uomo definisce "*necessity in a democratic society*" – in grado di assicurare un adeguato livello di garanzia dei diritti fondamentali alla riservatezza e protezione dei dati e che non sia regolato da una legge realmente prevedibile e conoscibile (criterio di "*foreseeability*").
L'ordinamento statunitense, unitamente alle tutele introdotte dal regime *Privacy Shield* (quali ad esempio l'istituzione della figura dell'Ombudsperson) non risultano, a seguito dell'analisi dettagliata dell'AG, predisporre strumenti di accesso alla giustizia e rimedi capaci di garantire il diritto sancito all'art. 47 della Carta di Nizza in maniera sostanzialmente equivalente a quanto stabilito nell'UE[20].
Pur tenendo conto della necessità di una certa «*flexibility in order to take various legal and cultural traditions into account*» (§ 249) nell'accertamento del livello di protezione garantito da uno Stato terzo e dunque della sua adeguatezza, l'Avvocato generale, al termine di una complessa disamina, esprime dubbi quanto alla conformità della decisione di adeguatezza 2016/1250 agli attt. 7, 8 e 47 della Carta di Nizza e all'art. 8 della Convenzione europea dei diritti dell'uomo.

3. Brevi considerazioni conclusive sui possibili sviluppi futuri: luci e ombre della disciplina europea in materia di trasferimento dati verso Stati terzi

Dai molteplici aspetti trattati dall'Avvocato generale e dalla complessità delle questioni giuridiche analizzate, è semplice comprendere come la Corte di giustizia si trovi dinnanzi ad un compito arduo, dalle delicate implicazioni sia sul piano economico che delle relazioni internazionali. L'esito finale di questa pronuncia ed i suoi effetti sono naturalmente ancora del tutto imprevedibili e del resto i giudici di Lussemburgo, in questioni attinenti alla tutela della privacy e protezione dei dati, non sono nuovi a distanziarsi dall'approccio più cauto dell'Avvocato generale[21]. Senza dubbio, se la decisione della Corte di giustizia dovesse seguire le indicazioni emerse dalle Conclusioni sopra esaminate, lo scenario potrebbe essere maggiormente favorevole per i *data exporter*, che in tal caso non vedrebbero intaccata la validità né delle SCCs indicate dalla Commissione né, con riferimento allo specifico flusso di dati con gli USA, dell'importante strumento della decisione di adeguatezza e del regime *Privacy Shield*. Il condizionale però è quanto mai d'obbligo. Anche in questa più vantaggiosa ipotesi, la

[20] Viene in tal sede criticata anche l'assenza di qualsiasi meccanismo di notifica ai soggetti sottoposti a misure di sorveglianza, anche quanto la messa a conoscenza non costituisce più un pericolo per il raggiungimento dell'obiettivo securitario: tale mancanza infatti renderebbe l'accesso ai rimedi eccessivamente difficile (§ 322). Quanto all'Ombudsperson, l'Avvocato generale dichiara di dubitare dell'abilità di tale meccanismo di compensare le carenze riscontrate nell'ordinamento statunitense.

[21] Per esempio nella nota sentenza *Digital Rights Ireland*, nonostante l'Avvocato generale avesse suggerito di modulare l'efficacia temporale della dichiarazione di invalidità della direttiva in materia di *data retention*, il giudice di Lussemburgo ha invece optato per un approccio più netto, ritenendo la normativa invalida sin dal momento della sua entrata in vigore.

situazione derivante rimarrebbe aperta ed indefinita, passibile dei più disparati epiloghi: non bisogna infatti sottovalutare il fatto che Saugmandsgaard Øe abbia rimandato a ciascun responsabile del trattamento e, in caso di sua inerzia, alle autorità di controllo nazionali il compito di effettuare valutazioni caso per caso circa la possibilità concreta di rispettare le clausole contrattuali dinnanzi agli obblighi stabiliti dall'ordinamento dello Stato ricevente. Non è quindi scontato e neppure certo che i singoli soggetti e autorità preposte a tale vaglio, con riferimento allo specifico regime di trasferimento posto alla loro attenzione, giungano a ritenere attuabili le SCCs, ben potendo propendere invece per una sospensione o divieto del flusso di dati stesso. Nel caso dal quale il rinvio pregiudiziale ha preso origine, ad esempio, la posizione espressa dal DPC irlandese al termine della propria indagine iniziale non sembra poter far tirare un sospiro di sollievo a Facebook, viste le numerose perplessità e preoccupazioni mostrate avverso le imposizioni derivanti dal sistema di sorveglianza statunitense e la loro compatibilità con il rispetto delle clausole contrattuale tipo inserite nell'accordo di trasferimento tra l'azienda irlandese e quella americana. Questa posizione dell'Avvocato generale apre dunque a molteplici scenari e alla possibilità che si addivenga a soluzioni differenti a seconda dei diversi approcci delle autorità di controllo degli Stati membri dinnanzi all'ordinamento degli Stati terzi "riceventi", che potrebbe peraltro variare nel corso del tempo.

Gli interrogativi che sorgono alla luce di queste considerazioni sono quindi numerosi: è da chiedersi innanzitutto se e come i responsabili del trattamento abbiano le forze, le capacità e l'interesse ad effettuare controlli così rilevanti quanto delicati, che implicano anche la conoscenza dell'ordinamento e dei vincoli normativi vigenti in ogni Stato ricevente. Queste valutazioni rimandano inevitabilmente alle critiche e perplessità emerse con riferimento alla posizione della Corte di giustizia nella nota sentenza *Google Spain* in materia di diritto all'oblio nonché nella più recente sentenza *Glawischnig-Piesczek*, sul controllo dei contenuti online[22]: attribuire un ruolo "para-costituzionale" a soggetti privati è veramente una strada percorribile, soprattutto quando interessi economici così rilevanti sono in gioco? Certamente, nel caso in esame, l'immobilismo dei *data exporter* può essere compensato dall'intervento delle autorità di controllo. Anche con riferimento a queste ultime però ci si domanda se esse siano dotate dei mezzi necessari per effettuare complesse e costanti valutazioni case-by-case, potenzialmente onerose sotto il profilo del tempo, sforzi e personale richiesti nonché particolarmente delicate per i risvolti economici che una sospensione comporterebbe; ciò anche considerando lo squilibrio e le disomogeneità che potrebbero venirsi a creare tra Stati membri a seconda dell'attivismo e delle decisioni delle diverse autorità nazionali, che potrebbero in ultima istanza portare anche ad uno spostamento dei server delle aziende negli Stati nei quali le autorità sono meno efficienti o effettuano un vaglio meno rigido. L'attribuzione di così ampi margini d'azione a soggetti privati o autorità di controllo e di una loro forte responsabilizzazione sembra scontare pertanto, ad una prima analisi, alcuni limiti e difficoltà pratiche sul piano della possibile concreta attuazione, tanto che non è mancato chi ha rinvenuto nella posizione espressa dall'Avvocato generale un «*a head in*

[22] CGUE, *Google Spain SL e Google Inc. v. Agencia Espanola de Proteccion de Datos e Mario Costeja Gonzalez,* C-131/12 (2014)*; Eva Glawischnig-Piesczek v. Facebook Ireland Limited*, C-18/18 (2019).

the sand approach»[23]. Infine, merita rilevare come in un tale contesto assumano un ruolo di centrale importanza, per quanto non menzionato nelle Conclusioni, l'attenzione e la vigilanza continue dimostrate dai comuni users di servizi digitali, al fine di segnalare ed attivare meccanismi di controllo in caso di inerzia dei *data controller* e delle autorità nazionali preposte. È innegabile infatti che dinnanzi alle difficoltà attuative sopra evidenziate potrebbe sopperire – in parte – un pubblico di utenti attivo ed informato. Anche sotto questo profilo, se una maggiore sensibilizzazione e, per certi versi anche responsabilizzazione, dell'utente i cui dati vengono trasferiti fuori dai confini europei è di grande rilievo, è altrettanto vero però che si rendono alla base necessarie adeguate conoscenze e competenze in materia: solo una approfondita consapevolezza innanzitutto dei meccanismi di raccolta, conservazione, trattamento e trasferimento dei propri dati da parte del soggetto cui li cediamo, nonché del sistema giuridico dello Stato ricevente e dell'esistenza di possibili obblighi in capo ai *data exporter* tali da intaccare la corretta attuazione e rispetto delle SSCs previste, potrebbe consentire al singolo utente di promuovere ricorsi per la tutela dei propri diritti. Come risulta evidente ciò risulta tutt'altro che semplice da realizzare.

Le difficoltà pratiche e la situazione confusa che ne potrebbe derivare, inducono dunque ad una lettura delle Conclusioni esaminati che vada al di là della mera affermazione di validità della decisione 2010/87/UE da parte dell'Avvocato generale: come sottolineato da alcuni primi commenti[24], l'approccio emerso non può essere considerato una vittoria a tutto tondo di Facebook o delle posizioni del governo statunitense, ben potendosi al contrario rivelare una vittoria di Pirro, nella quale i benefici si mostrano in conclusione assai limitati rispetto ai rischi corsi. Non è un caso se lo stesso Schrems si è dichiarato nel complesso soddisfatto delle considerazioni di Saugmandsgaard Øe che, è bene ricordarlo, ha finito col mostrare conclusivamente forti perplessità rispetto alla validità della decisione di adeguatezza e del relativo regime di Scudo per la privacy UE-USA, pur affrettandosi a precisare che le proprie considerazioni non hanno carattere di completezza. Con riferimento a tale aspetto, se la Corte dovesse decidere di non seguire il ragionamento ed i suggerimenti dell'Avvocato generale ed addentrarsi nella valutazione di questa decisione, potrebbe riproporsi nuovamente quella situazione di confusione ed incertezza già descritta per la fase post-*Schrems*: laddove l'invalidità fosse nuovamente dichiarata, la storia si ripeterebbe e si renderebbe necessaria una nuova complessa fase di rinegoziazione di principi e regole che disciplinino il trasferimento dati verso gli USA, accompagnati da una nuova decisione di adeguatezza. D'altra parte le considerazioni dell'Avvocato generale sulla inadeguatezza del livello di protezione dei dati e della riservatezza garantito dall'ordinamento statunitense e dall'accordo *Privacy Shield* paiono in linea con le criticità e problematiche sin da subito rilevate da parte della dottrina e da talune autorità europee[25], che già all'indomani della

[23] L. Woods, *The AG Opinion in Schrems II: Facebook, national security and data protection law*, in *EU Law Analysis*, 21 dicembre 2019.

[24] C. Kuner, *International data transfers, standard contractual clauses and the Privacy Shield: the AG Opinion in Schrems II*, in *European Law Blog*, 7 gennaio 2020.

[25] Si pensi alla posizione critica espressa dal Gruppo di lavoro Articolo 29, sia prima che dopo l'approvazione della decisione di adeguatezza (*Opinion 01/2016 on the draft EU-US Privacy Shield adequacy decision*, WP 238, 13 aprile 2016; *Press Release* del 1 luglio 2016, oltre alle *Annual Joint Review*

decisione della Commissione avevano evidenziato la mancata congruità e rispetto dei criteri indicati dalla giurisprudenza della Corte di giustizia nel caso *Schrems*, nonostante le positive modifiche apportate dagli Stati Uniti all'apparato regolatorio dei sistemi di sorveglianza massiva (si pensi al richiamato PPD 28) e le ulteriori tutele garantite dal regime di Scudo per la privacy (ad esempio i già evidenziati Ombudsman e l'estensione della vincolatività delle tutele previste nell'accordo anche alle autorità pubbliche americane).

Oltre a questi aspetti è importante poi rilevare come, nell'affrontare la questione relativa ai confini applicativi del diritto UE in materie connesse alla sicurezza nazionale, Saugmandsgaard Øe abbia fornito una chiave di lettura di grande importanza, pur non discostandosi dal passato e soprattutto da quanto affermato nelle sue Conclusioni nel caso *Ministerio Fiscal*. La posizione della Corte di giustizia sul punto sarà quindi determinante anche per i casi pendenti, sopra individuati, riguardanti la fondamentale quanto problematica disciplina della *data retention* per scopi securitari; la decisione finale inoltre potrà chiarire il rapporto tra il diritto europeo e la giurisprudenza della Corte europea dei diritti dell'uomo in questa materia: nel caso in cui venisse confermata la funzione "suppletiva" di quest'ultima rispetto alle attività di trattamento dei dati che fuoriescono dall'ambito di applicazione del diritto dell'UE, sarà poi interessante vedere se, alla luce delle altrettanto attese decisioni dei giudici di Strasburgo – in particolare nei casi *Big Brother Watch* e *Centrum for Rattvisa* – sarà confermata una interpretazione dei principi di necessità e proporzionalità meno stringente da parte della Corte europea dei diritti dell'uomo rispetto alla Corte di giustizia – come sottolineato peraltro dall'Avvocato generale[26] – o se si potrà individuare un maggiore allineamento tra la giurisprudenza delle due Corti europee.

In attesa di poter riflettere su questi determinanti sviluppi, ciò che senza dubbio affiora con chiarezza da tutte queste considerazioni sono le problematiche ed i limiti della normativa eurounitaria in materia di trasferimento dei dati: il criterio di adeguatezza muove dalla pregevole volontà di creare una continuità nel livello di protezione dei diritti fondamentali garantito entro i confini europei ed è stato portatore di positivi

del 28 novembre 2017 e del 22 gennaio 2019) o ai dubbi evidenziati dal Parlamento europeo nel 2018 (*European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield* (2018/2645(RSP)) e, prima ancora, dal European Data Protection Supervisor (*Opinion 4/2016,* 30 maggio 2016). Quanto alla dottrina, si rimanda a: G. Vermeulen, *The Privacy Shield's blunt denial of continued bulk, mass or indiscriminate collection or processing and unnecessary or disproportionate access and use by US intelligence and law enforcement authorities,* in G. Vermeulen-E. Lievens (eds.), *Data protection and privacy under pressure. Transatlantic tensions, EU serveillance and Big Data*, Antwerp, 2017, 49 ss.; S. Sica-V. D'Antonio, *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in G. Resta-V. Zeno Zencovich (a cura di), *La protezione transnazionale dei dati personali. Dai 'Safe Harbour Principles' al 'Privacy Shield',* cit., 137 ss. e, nella stessa opera, A. Mantelero, *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe harbour e Privacy Shield*, 239 ss.; S. Crespi, *op. cit.*; F. Terpan, *EU-US data transfer from Safe Harbour to Privacy Shield: back to square one?*, in *European Papers*, 3, 2018, 1045 ss.; M. Brkan, *The essence of the fundamental rights to privacy and data protection: finding the way through the maze of the CJEU's constitutional reasoning,* in *German Law Journal,* 20, 2019, 864 ss.

[26] Si rimanda sul punto anche a E. Celeste, *op. cit.*; V. Rusinova, *A European perspective on privacy and mass surveillance at the crossroads*, Working Papers HSE, 2019, 1 ss. Su *questa Rivista*, per un approfondimento sulla giurisprudenza della Corte europea dei Diritti dell'uomo in materia di sorveglianza: L. Seminara, *Sorveglianza segreta e nuove tecnologie nel diritto europeo dei diritti umani*, 2, 2018, 132 ss.

riflessi[27] sia inducendo modifiche o adozione di normative più garantiste negli Stati terzi interessati a ricevere i dati proveniente dall'UE, sia spingendo i service providers ad adottare policies interne in materia di privacy e protezione dei dati più attente ed efficaci per incontrare gli elevati standard europei[28]. Il tentativo però di sfruttare l'ormai imprescindibile flusso di dati come moderna forma di "*gunboat diplomacy*"[29] attraverso cui imporre unilateralmente agli Stati terzi il proprio grado di tutela reca in sé il rischio di tramutarsi in una mera «esaltante illusione»[30], smentita nella sua pratica attuazione: i principi delineati nella giurisprudenza della Corte di giustizia mostrano tutta la loro cedevolezza ed imperfezione negli accordi e nelle decisioni sin ad ora analizzati, incapaci di realizzare una reale "adeguatezza" e "sostanziale equivalenza" e di resistere dunque al successivo vaglio dei giudici europei. Ecco dunque che la ideale e condivisibile tensione dell'UE ad una garanzia della protezione che accompagni il dato anche oltre il suo trasferimento, si scontra con la difficoltà di negoziare principi e condizioni di tutela con Stati terzi portatori di tradizioni giuridiche e concezioni del livello di tutela della riservatezza anche molto differenti da quelle che caratterizzano le nostre latitudini[31].

Lo scenario di luci e ombre sino ad ora tratteggiato, al di là dei pregi e delle criticità evidenziate, permette in ultima analisi di riflettere da un lato sulla necessità di un'azione maggiormente coerente e condivisa tra le istituzioni europee, in modo che la posizione della Commissione nelle complesse fasi di trattativa con Paesi terzi non venga poi sconfessata dalla Corte di giustizia nelle sue pronunce, creando situazioni incerte e complesse per gli operatori economici ed incidendo anche sull'affidabilità dell'UE stessa nelle sue negoziazioni[32]; dall'altro emerge l'importanza di un serio dibattito internazionale, nel quale certamente l'Unione può risultare promotrice ed esempio trainante, per la creazione di uno standard globale di privacy e il raggiungimento di una convergenza regolatoria ottenuta mediante una cooperazione tra Stati tesa a garantire un sempre più elevato livello di tutela dei dati anche e soprattutto dinnanzi ad esigenze securitarie che tendono sempre più a limitare e sacrificare la sfera privata dei cittadini in nome della garanzia della sicurezza nazionale e pubblica[33].

---

[27] A. Bradford parla di *Brussels effect*, anche con riferimento all'effetto "espansivo" della disciplina in materia di riservatezza e protezione dei dati: *The Brussels effect*, in *Northwestern University Law Review*, 1, 2012, 22 ss.

[28] Basti pensare allo Stato della California che, in assenza di una normativa federale in materia di protezione dei dati, ha adottato nel 2018 il California Consumer Privacy Act (CCPA), chiaramente ispirato alla disciplina del GDPR; ma anche, sul fronte dei soggetti privati, aziende operanti nel settore digitale – ad esempio Microsoft – si sono attivate per adottare *policies* interne maggiormente conformi allo standard europeo.

[29] Espressione utilizzata da: M. Tzanou, *European Union regulation of transatlantic data transfers and online surveillance*, in *Human Rights Law Review*, 17, 2015, 545 ss.

[30] Questo efficace termine di L. Zagato (*Il trasferimento di dati personali verso Stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*, in *Diritto del commercio internazionale*, 2, 2008, 297 ss.) mette in luce i limiti di una imposizione unilaterale dei principi e livelli di tutela promossi dall'UE.

[31] Così C. Kuner, *Reality and illusion in EU data transfer regulation post-Schrems*, in *German Law Journal*, 18, 2017, 881 ss.

[32] J. Reidenberg, *The transparent citizen*, in *Loyola University Chicago Law Journal*, 47, 2015, 437 ss.

[33] *Ex multis*, sul dibattito circa la necessità di uno standard globale di protezione dei dati e della privacy,

Inserendosi in questo più ampio contesto, le Conclusione dell'Avvocato generale oggetto di esame nonché l'attesissima decisione della Corte di giustizia rappresentano certamente una occasione per interrogarci ancora una volta sulla efficacia della disciplina europea in materia di trasferimento dei dati e sulle problematiche profonde derivanti da una diversa attuazione ed interpretazione del criterio di adeguatezza ad opera delle istituzioni europee protagoniste in questo delicato ambito. I futuri sviluppi dovranno in ultima analisi indurre a profonde riflessioni circa il bilanciamento effettuato dai giudici di Lussemburgo tra utilizzo dei dati per esigenze securitarie e tutela della privacy, valutandone con attenzione le pratiche implicazioni sia nella dimensione esterna, e dunque con riferimento alla disciplina del flusso di dati, sia nella dimensione interna ovvero nelle complesse questioni in materia di *data retention*.

si legga: D. Cole-F. Fabbrini, *Bridging the transatlantic divide? The United States, The European Union and the protection of privacy across borders*, in *ICON*, 1, 2016, 220 ss.; S.J. Schulhofer, *An international right to privacy? Be careful what you wish for*, ivi, 238 ss.; C. Kuner, *The Internet and the global reach of EU law,* in M. Cremona-J. Scott (eds.), *EU law beyond EU borders. The extraterritorial reach of EU law*, Oxford, 2019, 112 ss.