ISSN 2384-9169
Fascicolo n. 1 - 2021
rivista.eurojus.it

La Corte di giustizia nega per la seconda volta la legittimità del trasferimento dei dati personali dall'Unione europea agli Stati Uniti senza una protezione "sostanzialmente equivalente" (*Schrems II*)

DI FLAVIA CALOPRISCO*

Sommario: 1. Il contesto della sentenza *Schrems II*. – 2. Il regime del trasferimento dei dati nel Regolamento 679/2016. – 3. Il conflitto regolatorio UE-USA in materia di protezione dei dati personali. – 4. L'invalidità del regime di protezione del *Privacy Shield* del 2016 alla luce della Carta dei diritti fondamentali. – 5. Il trasferimento di dati a seguito della sentenza *Schrems II*. – 6. Conclusioni.

1. Il contesto della sentenza *Schrems II*

La Corte di giustizia dell'Unione europea è tornata a pronunciarsi sul trasferimento dei dati personali verso gli USA, (*Schrems II*)[1], dichiarando invalida la decisione sull'adeguatezza della protezione offerta dal regime "scudo per la privacy" *(Privacy Shield*)[2] e affermando la validità delle clausole contrattuali standard (*Standard contractual clauses* o SCC) come meccanismo di trasferimento dei dati[3]. Non è la prima volta che la Corte è chiamata a giudicare

* Professore a contratto in diritto dell'Unione europea presso l'Università di Teramo, Dottore di ricerca in diritto dell'Unione europea con doppio titolo delle Università Paris-Est e Roma Tre, Avvocato presso il foro di Parigi.
[1] Corte di giustizia (Grande Sezione), 16 luglio 2020, causa C-311/18, EU:C:2020:559 ("*Schrems II*").
[2] Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione 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 d'America (in *GUCE*, L 215 del 25 agosto 2000, p. 7).
[3] Decisione 2010/87/UE della Commissione, del 5 febbraio 2010, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento stabiliti in paesi terzi a norma della direttiva 95/46 (in

la validità di una decisione della Commissione in materia. Infatti, nella sentenza *Schrems I*[4] la Corte aveva già dichiarato invalida la precedente decisione sull'adeguatezza relativa al regime di "approdo sicuro" (*Safe Harbor*)[5]. Nella sentenza la Corte aveva rilevato che una normativa che consente alle autorità pubbliche l'accesso in via generalizzata al contenuto di dati e comunicazioni elettroniche è potenzialmente in grado di compromettere l'*essenza del diritto fondamentale* al rispetto della vita privata[6].

A seguito della decisione *Schrems I*, la Commissione europea – dopo una nuova valutazione della normativa degli Stati Uniti e agli impegni[7] assunti al riguardo[8] – aveva adottato una seconda decisione di adeguatezza al fine di consentire i trasferimenti transnazionali dei dati attraverso lo strumento del *Privacy Shield*. La sentenza *Schrems II* consente così di consolidare il precedente orientamento giurisprudenziale nell'ambito di un procedimento che coinvolgeva le stesse parti (il *social network Facebook* e il ricorrente Sig. *Schrems* davanti all'Autorità garante per la *privacy* irlandese)[9]. Il ricorrente sosteneva che l'ordinamento statunitense continuava a non offrire protezione adeguata in relazione al ruolo "invasivo" dei programmi di *intelligence* e che i trasferimenti dei dati effettuati da *Facebook* tramite il ricorso alle clausole contrattuali standard[10] non garantivano una protezione adeguata. L'Autorità di

---

GUUE, L 39 del 12 febbraio 2010, p. 5), come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016 (in *GUUE*, L 344 del 17 dicembre 2016, p. 100).

[4] Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems*, ECLI:EU:C:2015:650 ("*Schrems I*").

[5] Decisione della Commissione, del 26 luglio 2000, cit. (in prosieguo: "approdo sicuro"); la circolazione dei dati personali extra-UE è soggetta al controllo tramite atti di esecuzione della Commissione ("decisioni di adeguatezza").

[6] Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit., punti 94 e 95. Nella sentenza *Schrems II*, cit. la Corte non esamina nuovamente la questione dell'essenza del diritto fondamentale alla protezione dei dati personali ma si limita a citare l'art. 23 RGPD. Tale articolo, al par. 11, stabilisce che: «Il diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o il responsabile del trattamento può limitare, mediante misure legislative, la portata degli obblighi e dei diritti […], qualora tale limitazione rispetti l'essenza dei diritti e delle libertà fondamentali e sia una misura necessaria e proporzionata […]». Sulla dottrina dell'"essenza dei diritti fondamentali", in rapporto con l'applicazione del principio di proporzionalità, v. vari contributi, in *German Law Journal, Special Issue, Essence of fundamental right in the EU*, tra cui: K. LENAERTS, *Limits on Limitations: The Essence of Fundamental Rights in the EU*, *ivi,* p. 779 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*, *ivi*, p. 864 ss.

[7] L'accordo *Privacy Shield* contiene principi, dichiarazioni e impegni assunti formalmente dall'Amministrazione degli Stati Uniti. Lo scudo prevede meccanismi di vigilanza e di controllo atti a verificare e garantire che le imprese statunitensi autocertificatesi come aderenti al regime rispettino i principi e che qualsiasi caso di inosservanza sia affrontato. Tali meccanismi sono illustrati negli allegati alla Decisione di esecuzione della Commissione 2016/1250 prec. e in particolare nei principi (allegato II) e negli impegni assunti dal Dipartimento del Commercio (allegato I), dalla Commissione federale del Commercio (FTC) (allegato IV) e dal Dipartimento dei Trasporti (allegato V).

[8] In particolare, si legge al punto 65 della decisione di adeguatezza che: «La Commissione ha valutato le limitazioni e le garanzie cui la normativa statunitense subordina la facoltà delle autorità pubbliche statunitensi di accedere e usare i dati personali trasferiti […] per soddisfare esigenze di sicurezza nazionale, amministrazione della giustizia o altro scopo d'interesse pubblico. […] Ai fini della trasparenza e per rispecchiare la natura giuridica di questi impegni, ciascuno dei documenti elencati e allegati alla presente decisione è pubblicato nel Registro federale degli USA».

[9] R.A. COSTELLO, *Everithing is illuminated?,* in *European Papers*, 2020, p. 1046 ss., disponibile all'indirizzo internet: https://www.europeanpapers.eu/en/europeanforum/schrems-II-everything-is-illuminated.

[10] A seguito della dichiarazione di invalidità del Safe Harbour Facebook, come molte altre società statunitensi, era passata alla base legale delle SCC per mantenere il flusso di dati dall'UE agli Stati Uniti. Le SCC sono contratti tra esportatori di dati dell'UE e importatori di dati non UE che mirano a regolamentare il trasferimento di dati tra i due soggetti, i rispettivi obblighi, responsabilità e i diritti che gli interessati possono esercitare nei confronti dell'esportatore e importatore di dati.

controllo irlandese (*Data Protection Commissioner* o *DPC*) ritenendo che la suddetta denuncia sollevava dubbi sulla validità della decisione della Commissione 2010/87/UE sulle SCC e della decisione di adeguatezza sul regime del *Privacy Shield*, presentava ricorso dinanzi alla *High Court* che, a sua volta, sospendeva il procedimento e sottoponeva alla Corte di giustizia un rinvio pregiudiziale con il quale venivano poste diverse questioni[11].

La recente vicenda si colloca in un contesto fattuale e giuridico radicalmente cambiato rispetto alla sentenza *Schrems I*[12]. In primo luogo, lo scandalo *Cambridge Analytica* ha fatto emergere le vulnerabilità delle misure di *privacy* di *Facebook* in relazione ad interferenze nelle elezioni democratiche. In secondo luogo l'Amministrazione Trump ha intrapreso politiche volte all'acquisizione di prove anche al di fuori degli Stati Uniti[13]. In terzo luogo, anche gli Stati membri dell'Unione hanno emanato leggi in risposta ad attacchi terroristici in favore di un modello improntato alle priorità della sicurezza nazionale.

2. Il regime del trasferimento dei dati nel Regolamento 679/2016

Ai sensi del Regolamento generale sulla protezione dei dati personali 679/2016 (di seguito "RGPD" o "Regolamento") i flussi di dati personali verso e da paesi al di fuori dell'Unione e organizzazioni internazionali sono necessari per l'espansione del commercio internazionale e della cooperazione internazionale. L'aumento di tali flussi ha posto nuove sfide e problemi riguardanti la protezione dei dati personali. Infatti, quando i dati personali sono trasferiti dall'Unione a titolari e responsabili del trattamento in Paesi terzi o a organizzazioni internazionali, è necessario che il livello di tutela nell'Unione sia assicurato anche in altri ordinamenti[14].

Al riguardo appare utile ricordare il quadro normativo che consente il trasferimento di dati extra-UE. Il Regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali comunque contenuti in un archivio. Ne consegue che il trasferimento da uno Stato membro verso un Paese terzo deve essere qualificato come un trattamento di dati personali[15].

---

[11] Il giudice del rinvio chiedeva alla Corte di giustizia undici questioni che possono riassumersi in cinque più ampie: se il RGPD si applica ai trasferimenti di dati quando è probabile che i dati vengano elaborati in un paese terzo per scopi di sicurezza; quale livello di protezione dei garantiscono le SCC e se tale livello di protezione deve essere letto in conformità con la Carta, la CEDU o la legislazione nazionale; se le SCC sono valide alla luce degli articoli 7, 8 e 47 della Carta; se le autorità nazionali per la protezione dei dati (DPA) sono tenute a sospendere o vietare i trasferimenti di dati ai sensi delle SCC se ritengono che le clausole non sono rispettate o il livello di protezione non può essere garantito; se lo Scudo per la privacy garantisce un livello adeguato di protezione dei dati trasferiti.

[12] F. BIGNAMI, *Schrems II: The Right to Privacy and the New Illiberalism*, in *Verfassungsblog*, 29 luglio 2020, disponibile all'indirizzo internet: https://verfassungsblog.de/schrems-ii-the-right-to-privacy-and-the-new-illiberalism/.

[13] Il *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) consente alle autorità statunitensi, forze dell'ordine e agenzie di intelligence di acquisire dati informatici dagli operatori di servizi di *cloud computing* a prescindere dal posto dove questi dati si trovano; cioè anche su server fuori dagli Usa. La sola condizione è che questi operatori siano sottoposti alla giurisdizione degli Stati Uniti oppure siano le società europee che hanno una filiale negli Stati Uniti o che operano nel mercato statunitense.

[14] Considerando 101, RGPD.

[15] L'articolo 4, punto 2, RGPD definisce la nozione di «trattamento» come «qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali» e menziona, a titolo esemplificativo, «la comunicazione mediante trasmissione, diffusione o qualsiasi

In coerenza con la sua giurisprudenza[16], la Corte ha statuito che i trasferimenti di dati personali effettuati da parte di un operatore economico a fini commerciali, anche se tali dati personali sono successivamente trattati dalle Autorità di controllo dello Stato di destinazione per motivi di sicurezza nazionale, rimangono nell'ambito di applicazione del RGPD. A tal proposito la Corte ha rilevato che

il fatto che l'art. 4, par. 2 del TUE ha posto le questioni di sicurezza nazionale nella competenza esclusiva degli Stati membri non influisce sull'applicabilità del RGPD[17].

Ai sensi del Regolamento[18], il trasferimento può avvenire solo se il Paese in questione garantisce un adeguato livello di protezione[19]. Tale livello è oggetto di valutazione da parte della Commissione in relazione alla legislazione nazionale o agli impegni internazionali assunti dal Paese terzo[20]. In realtà più che alla "adeguatezza" la Corte di giustizia e il RGPD[21], fanno riferimento alla protezione "sostanzialmente equivalente"[22]. In altri termini, il Paese terzo dovrebbe offrire garanzie di protezione dello stesso livello di quelle assicurate all'interno dell'Unione[23]. In particolare, il Paese dovrebbe assicurare un effettivo controllo di un'autorità indipendente e dovrebbe prevedere meccanismi di cooperazione con le autorità di protezione dei dati degli Stati membri. Inoltre, agli interessati dovrebbero essere riconosciuti diritti azionabili tramite un mezzo di ricorso effettivo in sede amministrativa e giudiziale. In mancanza di una decisione di adeguatezza sul livello di protezione offerta dal Paese terzo, un trasferimento può essere effettuato solo se l'esportatore dei dati personali prevede garanzie adeguate. Siffatte

---

altra forma di messa a disposizione», senza distinguere a seconda che tali operazioni siano realizzate all'interno dell'Unione o presentino un nesso con un paese terzo.

[16] Corte giust., 29 luglio 2019, causa C-40/17, *Fashion ID GmbH & Co. KG*, ECLI:EU:C:2019:629.

[17] Corte giust., 16 luglio 2020, causa C-311/18, *Schrems II*, cit., punto 81, in cui la Corte non ha distinto, come aveva fatto l'Avvocato generale tra "trattamento consistente nel trasferimento stesso" e successivo trattamento da parte delle autorità di sicurezza nazionale di un paese terzo (si veda il punto 104 delle conclusioni), ritenendo così che la possibilità di tale il successivo trattamento non fosse rilevante alla luce dell'art. 45 RGPD. A tal proposito si veda il paragrafo 87.

[18] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.

[19] In tale contesto, il considerando 107 del RGPD enuncia che, allorché «un paese terzo, un territorio o un settore specifico all'interno di un paese terzo (...) non garantiscono più un livello adeguato di protezione dei dati (...) il trasferimento di dati personali verso tale paese terzo (...) dovrebbe essere vietato, a meno che non siano soddisfatti i requisiti di cui [a tale regolamento] relativamente ai trasferimenti sottoposti a garanzie adeguate».

[20] Articolo 45, RGPD.

[21] Cfr. considerando 104, RGPD.

[22] Nella sentenza *Schrems I*, cit., punti 73-74, la Corte di giustizia ha chiarito che l'espressione "livello di protezione adeguato" figurante all'articolo 25, paragrafo 6, della direttiva 95/46/CE, pur non implicando un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, deve essere intesa nel senso che esige che il paese terzo assicuri un livello di protezione delle libertà e dei diritti fondamentali "sostanzialmente equivalente" a quello garantito all'interno dell'Unione in forza della direttiva 95/46/CE, letta alla luce della Carta dei diritti fondamentali. Anche se gli strumenti dei quali tale paese terzo si avvale al riguardo possono essere diversi da quelli attuati all'interno dell'Unione, tali strumenti devono cionondimeno rivelarsi efficaci nella prassi. Nella sentenza *Schrems II*, cit., punto 94, la Corte ribadisce il concetto di protezione adeguata: «A tal riguardo, senza esigere che il paese terzo considerato garantisca un livello di protezione identico a quello garantito nell'ordinamento giuridico dell'Unione, l'espressione "livello di protezione adeguato" deve essere intesa, come confermato dal considerando 104 dello stesso regolamento, nel senso che esige che tale paese assicuri effettivamente, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito all'interno dell'Unione in forza di tale regolamento, letto alla luce della Carta».

[23] I paesi terzi non sono obbligati ad adottare uno standard di protezione identico, ma gli individui devono comunque godere di un grado di protezione "sostanzialmente equivalente" a quello offerto dal diritto dell'Unione (Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit., punto 73).

garanzie possono risultare, in particolare, dall'adozione di clausole standard di protezione dei dati adottate dalla Commissione[24]. Peraltro, in mancanza di una decisione di adeguatezza o di garanzie adeguate, il RGDP stabilisce ulteriori condizioni attraverso le quali può avvenire un trasferimento sulla base dei motivi di deroga[25].

In questo quadro, il crescente "ruolo costituzionale della Corte di giustizia"[26] può affermare nel contesto internazionale un modello europeo di protezione dei dati personali[27] che sia espressione dei suoi valori e del giusto bilanciamento tra esigenze di tutela dei diritti fondamentali e dell'interesse pubblico alla sicurezza. Appare evidente che i modelli giuridici di protezione della *privacy* di Stati Uniti e Unione sono di non facile conciliazione[28]. Il tema della legittimità del trasferimento internazionale dei dati e dell'applicabilità extraterritoriale della legislazione dell'Unione solleva la questione della sua "sovranità digitale". Tale questione rappresenta un *asset* strategico per le relative politiche dell'Unione europea dal momento che "il mercato digitale rappresenta una fascia ad elevato valore aggiunto per i cittadini e le imprese"[29]. A tal proposito l'applicabilità territoriale del diritto dell'Unione europea in materia di protezione dei dati personali è stata già affrontata dalla Corte di giustizia nella sentenza *Google Spain*[30] con un'interpretazione evolutiva[31] ed è stata poi codificata nel RGPD[32]. In tale ambito un'importante novità è l'introduzione del concetto di *targeting* degli utenti dei servizi digitali in relazione alle imprese straniere che offrono beni o servizi o effettuano il "monitoraggio" del comportamento di residenti europei[33].

3. Il conflitto regolatorio UE-USA in materia di protezione dei dati personali

La sentenza *Schrems II* sviluppa la posizione ormai consolidata dalla Corte di giustizia contro la sorveglianza tecnologica di massa in continua espansione[34]. Come è noto la protezione dei dati personali non è solo un diritto fondamentale individuale, ma coinvolge anche un interesse pubblico, una garanzia per la vita democratica e, dunque, per i valori su cui si fonda l'Unione.

---

[24] Articolo 46, paragrafo 1 e paragrafo 2, lettera c), del RGPD.

[25] Articolo 49 del RGPD.

[26] G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *Studi sull'integrazione europea*, 2018, p. 9 ss.

[27] A. BRADFORD, *The Brussels Effect and the International Order*, in https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?article=1275&context=faculty_scholarship.

[28] J. WHITMAN, *The Two Western Cultures of Privacy: Dignity v. Liberty,* in *The Yale Law Journal*, 2004, p. 1151 ss.

[29] COM (2015) 550 final, 28 ottobre 2015, Migliorare il mercato unico: maggiori opportunità per i cittadini e per le imprese.

[30] Corte giust., 13 maggio, 2014, causa C-131/12, *Google Spain c. Agencia Española de Protecciòn de Datos, Costeja*, ECLI:EU:C:2014:317.

[31] G. CAGGIANO, *L'interpretazione del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali,* in *Diritto dell'informazione e dell'informatica*, 2014, p. 605 ss.

[32] Art. 3, RGPD.

[33] EDPB, Linee-guida 3/2018 sull'ambito di applicazione territoriale del RGPD (articolo 3), Versione 2.1, 12 novembre 2019.

[34] G. CHUCHES; M. ZALNIERIUTE, *A Groundhog Day in Brussels: Schrems II and Internat\ta Transfers, Verfassungslog*, 16 luglio 2020, disponibile all'indirizzo internet: https://verfassungsblog.de/a-groundhog-day-in-bruessels/.

Le serie minacce alla sicurezza nazionale autorizzano raccolte generali o mirate di dati ma sono necessarie garanzie per i cittadini quali la limitazione temporale della raccolta dati e il controllo giudiziario o di un'autorità amministrativa indipendente. Lo svolgimento del ruolo della Corte di giustizia non solo a livello europeo ma anche a livello globale, garantisce in particolare il giusto equilibrio degli interessi in gioco attraverso la valutazione della necessità e proporzionalità delle misure adottate. A tal riguardo, il riconoscimento della Carta dei diritti fondamentali come fonte di diritto primario ha dato un contributo decisivo agli ultimi sviluppi della giurisprudenza in materia di dati personali[35].

Nei rapporti giuridici transatlantici la situazione dell'ordinamento statunitense esprime una diversa concezione in materia. Ciò che emerge dalla sentenza *Schrems II* è che il diritto statunitense impone a F*acebook Inc*. di mettere a disposizione delle autorità pubbliche, quali la *National Security Agency* ("NSA") e le *Federal Bureau of Investigation* ("FBI"), i dati personali che sono loro trasferiti. Secondo la Corte di giustizia tali dati sono utilizzati nell'ambito di diversi programmi di sorveglianza in modo incompatibile con gli articoli 7, 8, e 47 della Carta[36]. Per altri aspetti relativi ai programmi di sicurezza delle agenzie, la Corte si limita per mancanza di competenza[37] a rimandare alle analisi contenute nella decisione della *Irish Court*[38].

4. L'invalidità del regime di protezione del *Privacy Shield* del 2016 alla luce della Carta dei diritti fondamentali

Il ruolo costituzionale della Corte di giustizia si esprime prioritariamente nel bilanciamento fra il diritto fondamentale alla protezione dei dati personali e l'interesse pubblico

---

[35] F. BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali,* in *Diritto dell'Unione europea,* 2015, p. 21 ss.

[36] Nei considerando da 67 a 124 della decisione «scudo per la privacy», la Commissione fa riferimento alla possibilità che le autorità pubbliche statunitensi accedano ai dati trasferiti dall'Unione e li utilizzino a fini di sicurezza nazionale nell'ambito di programmi basati, in particolare, sull'articolo 702 del FISA o sull'Executive Order n. 12333.

[37] Il tema della sicurezza nazionale e del suo rapporto con il diritto dell'Unione è di grande attualità non solo perché è al centro del dibattito politico di diversi Stati membri, ma anche in quanto interferisce con la tutela dei diritti e delle libertà fondamentali di cui diffusamente si discute nell'attuale fase di evoluzione dell'Unione. Sul tema della competenza esclusiva degli Stati membri in materia di sicurezza nazionale si veda *ex multis*: H.J. BLANKE, *Article 4 The relations Between the EU and the Member States*, in H.J. BLANKE, S. MANGIAMELI (eds.), *The Treaty on European Union (TEU)*, Berlin, 2013, p. 229 ss.; G. MARTINICO, *What Lies Behind Article 4(2) TEU*?, in A. SÁIZ ARNAIZ, C. ALCOBERRO LLIVINA (eds.), *National constitutional identity and european integration*, Cambridge, 2013, p. 93 ss.; F. FERRARO, *Brevi note sulla competenza esclusiva degli Stati membri in materia di sicurezza nazionale*, in *AISDUE*, 2019, p. 95 ss.

[38] Il giudice del rinvio precisa, che, al fine di procurarsi «informazioni in materia di intelligence esterna», la legislazione statunitense consente al procuratore generale e al direttore dell'intelligence nazionale di autorizzare congiuntamente, previa approvazione della *Foreign Intelligence Surveillance Court* ("FISC"), la sorveglianza di cittadini stranieri che si trovano al di fuori del territorio degli Stati Uniti e serve, in particolare (a fondamento in particolare, dei programmi di sorveglianza PRISM e UPSTREAM). Nell'ambito del programma PRISM, i fornitori di servizi Internet sono tenuti, secondo le constatazioni di tale giudice, a fornire alla NSA tutte le comunicazioni inviate e ricevute da un «selettore», e parte di esse è trasmessa anche allo FBI e alla *Central Intelligence Agency* (CIA) (agenzia centrale per l'intelligence). Per quanto riguarda il programma UPSTREAM, lo stesso giudice ha constatato che, nell'ambito di tale programma, le imprese di telecomunicazioni che gestiscono la «dorsale» di Internet – vale a dire la rete di cavi, commutatori e router – sono costrette a consentire alla NSA di copiare e filtrare i flussi di traffico Internet al fine di raccogliere comunicazioni inviate da, dirette a o riguardanti il cittadino straniero interessato. Nell'ambito di tale programma, la NSA, avrebbe accesso tanto ai metadati quanto al contenuto delle comunicazioni interessate.

alla sicurezza nazionale interpretato alla luce della Carta[39]. Nella sentenza *Schrems II* la Corte utilizza quale parametro di legittimità della decisione di adeguatezza della Commissione gli articoli 7, 8, 47 e 52, della Carta[40]. Infatti una decisione che riconosce un "livello di protezione adeguato" alla legislazione di un Paese terzo deve essere interpretato in relazione alla Carta e in particolare in ossequio al principio di proporzionalità[41] e al diritto a un ricorso effettivo[42].

Nella sentenza, la Corte di giustizia ha affermato la validità della decisione della Commissione che adotta le clausole contrattuali standard come meccanismo di trasferimento dei dati, ma con alcune condizioni: l'esportatore dei dati è tenuto a valutare la capacità dell'importatore di dati di rispettare gli accordi contrattuali incorporati nelle SCC e addurre "garanzie aggiuntive" ove appropriato[43]. La validità delle clausole contrattuali standard dipende dal fatto che includono "meccanismi efficaci che consentono, nella pratica, di garantire il rispetto del livello di protezione richiesto dal diritto dell'UE[44] e che i trasferimenti di dati personali ai sensi delle SCC sono sospese o vietate da parte dell'autorità di controllo in caso di violazione di tali clausole o di impossibilità di rispettarle[45].

La Corte ha invece statuito l'invalidità della decisione di adeguatezza del regime di protezione del *Privacy Shield*. I motivi alla base della declaratoria di invalidità sono indicati dalla Corte: *i)* la mancanza delle necessarie limitazioni e garanzie sul potere delle autorità pubbliche ai sensi della legge statunitense in particolare il principio di proporzionalità; *ii)* la mancanza di rimedi giurisdizionali efficaci esperibili da parte dei cittadini dell'Unione e in generale le carenze del regime di protezione offerto dallo scudo per la privacy[46]. Infatti per soddisfare il requisito di proporzionalità, la normativa deve prevedere regole chiare e precise sulla portata e l'applicazione della misura garantendo così che l'ingerenza sia limitata allo stretto necessario. La Corte considera che i programmi di sorveglianza statunitensi non sono limitati allo stretto necessario. Infatti, l'ordinamento giuridico americano non autorizza singole

---

[39] G. CAGGIANO, *La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali*, in *AISDUE,* 2018, p. 9 ss. La Corte afferma nella sentenza *Schrems I*, cit., punto 60 che «l'Unione è un'Unione di diritto, nel senso che tutti gli atti delle sue istituzioni sono soggetti al controllo della conformità, segnatamente, ai Trattati, ai principi generali del diritto nonché ai diritti fondamentali […]». Le decisioni della Commissione adottate in forza dell'articolo 25, paragrafo 6, della direttiva 95/46 non possono pertanto sfuggire ad un siffatto controllo. G. CAGGIANO, *Sul trasferimento internazionale dei dati*, cit.

[40] Corte giust., 16 luglio 2020, causa C-311/18, *Scherms II*, cit., punti 170-176. Sulla Carta quale parametro di validità e interpretazione si veda F. BESTAGNO, *Validità e interpretazione degli atti dell'UE alla luce della Carta*, cit.; ID., *I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia*, in *Diritti umani e diritto internazionale*, 2015, p. 259 ss.

[41] Articolo 52, paragrafo 1 della Carta. Con riferimento all'applicazione del principio di proporzionalità nel giudizio sui diritti in generale per tutti si vedano: R. ALEXY, *Teoria dei diritti fondamentali*, Bologna, 2012; A. BARAK, *Proportionality*, Cambridge, 2012.

[42] Articolo 47 della Carta.

[43] Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit.

[44] Le SCC includono l'obbligo delle parti di verificare, prima del trasferimento, se il livello di protezione garantito dalle SCC possa essere rispettato nel paese terzo in questione (SCC, Clausola 4 (a) e Clausola 5 (a) e (b)), l'obbligo dell'importatore di dati di informare l'esportatore di dati della sua incapacità di rispettare le SCC (clausola 5 (a)) e di qualsiasi "richiesta legalmente vincolante di divulgazione dei dati personali da parte di un'autorità di contrasto se non diversamente proibito" (Clausola 5 (d) (i)), e il diritto del titolare del trattamento di sospendere il trasferimento dei dati o risolvere il contratto qualora il destinatario dei dati non sia più in grado di adempiere agli obblighi contrattuali di cui alle SCC (Clausola 5 (a) e (b)).

[45] Corte giust., 16 luglio 2020, causa C-311/18, *Schrems II*, cit., punti 135-137.

[46] Corte giust., 16 luglio 2020, causa C-311/18, *Schrems II*, cit., punti 193-197.

misure di sorveglianza ma programmi generalizzati. Una tale legislazione viola il principio di proporzionalità[47].

Riguardo alla tutela giurisdizionale, la sentenza prosegue analizzando la figura del Mediatore istituito dal *Privacy Shield* in relazione alle garanzie previste dall'art. 47 della Carta[48]. A tal proposito la Corte ha sottolineato che l'istituzione del Mediatore non fornisce una protezione sostanzialmente equivalente a quella dell'Unione. Infatti i cittadini dell'Unione non hanno accesso agli stessi mezzi di ricorso di cui dispongono i cittadini statunitensi contro i trattamenti di dati personali da parte delle autorità pubbliche. I ricorsi che restano a disposizione incontrano notevoli ostacoli, in particolare in ragione dell'obbligo di dimostrare la legittimazione ad agire.

Il meccanismo di mediazione previsto dal *Privacy Shield* non istituisce un organo indipendente in ragione del fatto che il Mediatore deve riferire al Segretario di Stato americano e che non ha il potere di prendere decisioni vincolanti riguardo ai servizi di *intelligence*[49]. Inoltre il Mediatore è designato dal Segretario di Stato e costituisce parte integrante del Dipartimento di Stato degli Stati Uniti e il *Privacy Shield* non contiene alcuna indicazione circa le garanzie sulla revoca del suo mandato. Tale circostanza è idonea a mettere in dubbio l'indipendenza stessa del Mediatore rispetto al potere esecutivo. Pertanto, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenerne la rettifica o la cancellazione, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta[50].

Il parametro dell'adeguatezza viene inteso dalla Corte nel senso di "equivalenza sostanziale" implicando un confronto diretto tra la protezione dei dati garantita dall'Unione e quella degli Stati Uniti. La Corte ha rilevato che la legislazione statunitense[51] non garantisce un livello di protezione sostanzialmente equivalente in quanto il suo programma di sorveglianza ai fini d'*intelligence* non include alcuna limitazione o garanzia per i cittadini dell'Unione, i cui diritti non sono di fatto azionabili in tribunale[52].

Sulla base di queste considerazioni, la Corte ha statuito che la decisione d'adeguatezza sulla quale poggia il *Privacy Shield* è incompatibile con i requisiti previsti dal Regolamento[53], ai sensi della Carta. Ne discende l'invalidità dell'atto nella sua interezza. Si tratta invece della

---

[47] Corte giust., 16 luglio 2020, causa C-311/18, *Schrems II*, cit., punto 185.

[48] Per quanto attiene, all'articolo 47 della Carta, che è anch'esso parte del livello di protezione richiesto all'interno dell'Unione e il cui rispetto deve essere constatato dalla Commissione prima di adottare una decisione di adeguatezza ai sensi dell'articolo 45, paragrafo 1, del RGPD, occorre ricordare che il primo comma di tale articolo 47 esige che ogni persona - i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati - abbia diritto a un ricorso effettivo dinanzi a un giudice nel rispetto delle condizioni previste da tale articolo. Ai sensi del secondo comma di tale articolo, ogni persona ha diritto a che la sua causa sia esaminata da un giudice indipendente e imparziale.

[49] Corte giust., 16 luglio 2020, causa C-311/18, *Scherms II*, cit., punti 187-197.

[50] Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit., punto 95.

[51] In particolare, la sezione 702 del *Foreign Intelligence Surveillance Act* ("FISA").

[52] Corte giust., 16 luglio 2020, causa C-311/18, *Scherms II*, cit., punti 178-182.

[53] Il RGPD assoggetta i trasferimenti di dati personali verso paesi terzi a norme specifiche contenute nel suo capo V, intitolato «Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali».

terza volta in cui, la Corte procede alla dichiarazione di invalidità di un atto di diritto derivato in materia di protezione dei dati personali[54].

La sentenza dimostra il rilievo attribuito dalla Corte al diritto fondamentale alla protezione dei dati in un mondo in cui la sorveglianza è sempre più generalizzata.

Peraltro, in alcune sentenze recenti e in particolare nelle sentenze *Digital Rights Ireland*[55] e *Schrems I*[56], la Corte di giustizia ha già affrontato il problema del giusto equilibrio tra diritto alla protezione dei dati personali e sicurezza pubblica, in applicazione del principio di proporzionalità al contempo come parametro di validità e fondamento stesso del diritto alla protezione dei dati personali. Nella prima sentenza la Corte ha dichiarato invalida la direttiva del 2006 ("direttiva *Data retention*")[57] in materia di conservazione dei dati di traffico telefonico e telematico per violazione del principio di proporzionalità. Nella seconda sentenza la Corte ha statuito l'invalidità della decisione di adeguatezza della Commissione europea[58] per violazione del contenuto essenziale del diritto alla protezione dei dati personali. A tal riguardo se il contenuto essenziale del diritto è messo in discussione, la limitazione dev'essere considerata illegittima senza che occorra valutare ulteriormente se risponda a una finalità di interesse generale e soddisfi i requisiti di necessità e di proporzionalità[59]. La necessità di disporre di siffatte garanzie è tanto più importante allorché i dati personali sono soggetti a un trattamento automatizzato[60].

5. Il trasferimento di dati a seguito della sentenza *Schrems II*

La sentenza ha una particolare importanza per le imprese del Mercato digitale e per le stesse autorità di controllo. Infatti venendo meno il *Privacy Shield*, il ricorso alle SCC e alle norme vincolanti d'impresa ("*Binding corporate rules"* o "BCR")[61] per legittimare il trasferimento avrà un ruolo sempre più importante. A differenza delle conclusioni raggiunte in *Schrems I*, in *Schrems II* la Corte di giustizia non solo ha invalidato la decisione di adeguatezza su cui era fondato il *Privacy Shield* che consentiva il trasferimento di dati verso Stati Uniti, ma

---

[54] Corte giust., 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a.*, ECLI:EU:C:2014:238 e 6 ottobre 2015, causa C-362/14, *Schrems I*, cit.

[55] Corte giust., 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland e Seitlinger e a.*, cit.

[56] Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, cit.

[57] La direttiva 2006/24/CE obbligava i fornitori di servizi di comunicazione elettronica a conservare i dati relativi al traffico e i dati relativi all'ubicazione per un periodo non inferiore a sei mesi e non superiore a 24 mesi, e a permettere alle autorità nazionali competenti di accedere a tali dati a fini di prevenzione, indagine, accertamento e perseguimento di reati gravi.

[58] La Corte di giustizia ha dichiarato invalida la decisione n. 2000/250 della Commissione europea, la quale consentiva il trasferimento dati personali di cittadini europei verso gli Stati Uniti.

[59] Necessity Toolkit, Bruxelles, 11 aprile 2017, disponibile all'indirizzo internet: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf.

[60] Corte giustizia, Parere sull'Accordo PNR UE-Canada, del 26 luglio 2017, EU:C:2017:592, paragrafo 139.

[61] Le BCR prevedono ai sensi dell'art. 47, RGPD che vengano fissati in norme vincolanti d'impresa i requisiti minimi quali l'indicazione della struttura organizzativa del gruppo imprenditoriale, i trasferimenti di dati previsti, le regole che l'organizzazione ritiene giuridicamente vincolanti, la dichiarazione su come si intenda applicare i principi base di protezione, i diritti dei soggetti interessati, il riconoscimento di potenziali responsabilità per le eventuali violazioni, il monitoraggio interno rispetto alla *compliance*, la comunicazione con i soggetti interessati e la cooperazione con le autorità. L'approvazione delle BCR da parte delle autorità di controllo prevede una procedura lenta e onerosa.

ha anche sottolineato che lo stesso standard di protezione dovrebbe essere garantito quando il trasferimento è operato attraverso gli altri mezzi previsti dal RGPD[62].

Come ulteriormente chiarito dal Comitato europeo per la protezione dei dati (di seguito *European Data Protection Board* o EDPB) nelle sue FAQ[63] sulla sentenza *Schrems II,* lo standard di protezione richiesto dalla Corte si applica anche a tutte le garanzie adeguate[64] utilizzate per legittimare il trasferimento dei dati dall'Unione verso un Paese terzo.

A riguardo la Corte dichiara infatti che l'invalidità del *Privacy Shield* non crea un vuoto giuridico nella misura in cui esistono altri meccanismi, come le SCC elaborate dalla Commissione, che possono a determinate condizioni consentire il trasferimento internazionale dei dati[65]. Tuttavia, tali clausole non si riferiscono ad uno specifico Paese terzo ma si limitano a individuare le fattispecie astrattamente idonee a garantire un adeguato livello di tutela. Pertanto, sarà oggetto di valutazione caso per caso a cura dell'esportatore dei dati se il trasferimento necessita di garanzie supplementari. In tal modo, è necessario verificare se il Paese terzo garantisce effettivamente un livello adeguato di protezione dei dati. Se ciò non avviene, l'esportatore deve interrompere il trasferimento.

Inoltre la Corte di giustizia suggerisce la possibilità che, anche se le leggi del paese dell'importatore non offrono un livello "adeguato" di protezione in relazione all'accesso del governo ai dati, i trasferimenti internazionali possono comunque aver luogo se l'importatore dei dati mette in atto "misure supplementari" "garanzie aggiuntive" o "misure aggiuntive" o "meccanismi efficaci per renderlo possibile nella pratica[66] per garantire la protezione dei dati trasferiti con altri mezzi[67].

A tal riguardo si configura una responsabilizzazione in capo al soggetto esportatore dei dati (titolare o responsabile) che deve valutare caso per caso se vi siano le condizioni per il trasferimento sotto la vigilanza delle autorità nazionali di controllo. Si tratta di una sorta di "privatizzazione della *governance* digitale" secondo la quale si ritiene che funzioni meglio il controllo dei medesimi soggetti che vi operano[68].

La Corte ha inoltre precisato che è ancora possibile utilizzare le BCR e a determinate condizioni le deroghe previste dal RGPD[69]. In particolare, quando i trasferimenti sono basati

---

[62] I. OLDANI, *The future of data trasfert rules in the aftermath of Schrems II*, in *SIDIBlog*, 23 ottobre 2020, disponibile all'indirizzo internet: http://www.sidiblog.org/2020/10/23/the-future-of-data-transfer-rules-in-the-aftermath-of-schrems-ii/.

[63] EDPB, *Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems*, 23 luglio 2020, https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf.

[64] Ai sensi dell'art. 46 RGPD.

[65] Corte giust., 16 luglio 2020, causa C-311/18, *Scherms II*, cit., punto 202.

[66] *Ivi*, punti 133, 134, 135 e 137.

[67] A tal fine la Corte si riferisce al Considerando 109 del RGPD che prevede l'uso di «altre clausole e garanzie aggiuntive» in casi in cui le clausole contrattuali standard non possono garantire la protezione.

[68] Tesi riconosciuta dalla giurisprudenza della Corte di giustizia quando ha affidato ai motori di ricerca (sentenza *Google Spain*) un ruolo di bilanciamento fra diritti fondamentali (*privacy* e diritto all'informazione) nella deindicizzazione dei dati per il diritto all'oblio, così come quando ha incaricato i medesimi gestori privati per la rimozione, a determinate condizioni, dei contenuti online (sentenza *Glawischnig-Piesczek*). A tal proposito si vedano le sentenze del 13 maggio 2014, causa C-131/12*, Google Spain SL.*, ECLI:EU:C:2014:317; del 24 settembre 2019, causa C-507/17, *Google LLC c. CNIL*, ECLI:EU:C:2019:772; e del 3 ottobre 2019, causa C-18/18, *Eva Glawischnig-Piesczek*, ECLI:EU:C:2019:821.

[69] Deroghe previste ai sensi dell'art. 49 RGPD. A tal proposito si vedano le Linee-guida del comitato europeo per la protezione dei dati 2/2018 sulle deroghe di cui all'articolo 49 del regolamento (CE) n. 2016/679, adottate il 25

sul consenso dell'interessato, esso dovrebbe essere esplicito, specifico con riguardo al particolare trasferimento o insieme di trasferimenti e informato, in particolare sui possibili rischi del trasferimento verso un Paese terzo che non fornisce una protezione adeguata.

Il RGPD prevede altre possibili basi giuridiche per trasferire i dati. Per quanto riguarda l'esecuzione di un contratto occorre tenere presente che i dati personali possono essere trasferiti solo su base occasionale. In relazione ai trasferimenti necessari per importanti motivi di interesse pubblico (che devono essere riconosciuti nella legislazione dell'UE o degli Stati membri), l'EDPB ricorda che il requisito essenziale per l'applicabilità di tale deroga è la constatazione della sussistenza di importanti motivi di interesse pubblico, e non già la natura del soggetto coinvolto nel trasferimento[70]. Inoltre sebbene tale deroga non sia limitata ai trasferimenti di dati aventi natura "occasionale", ciò non significa che i trasferimenti di dati sulla base della deroga relativa alla sussistenza di importanti motivi di interesse pubblico possano configurarsi su larga scala e in modo sistematico[71].

La sentenza *Schrems II* ha inoltre sottolineato la centralità delle autorità di controllo di ciascun Stato membro. Infatti le stesse sono chiamate a garantire che gli esportatori dei dati adottino tutte le misure idonee a garantire il rispetto del RGPD[72]. Le autorità di controllo, anche attraverso il sistema della *Leading Authority* e del meccanismo di coerenza, devono intervenire ove il trasferimento dei dati si riveli in violazione al RGPD, potendo disporre il blocco di tali trasferimenti. Pertanto, l'autorità di controllo deve indagare su una denuncia o d'ufficio circa le misure di garanzia adottate per il trasferimento. Ne discende che una decisione di adeguatezza della Commissione[73] o l'utilizzo delle SCC non può impedire alle persone i cui dati personali sono stati o potrebbero essere trasferiti verso un Paese terzo di investire di un reclamo[74] l'autorità nazionale di controllo. Di conseguenza ciascuna delle autorità è investita della competenza di verificare se un trasferimento di dati personali dallo Stato membro a cui essa appartiene verso un Paese terzo rispetti i requisiti stabiliti dal RGPD[75] e deve sottoporre, secondo il diritto processuale nazionale, la questione dinanzi ai tribunali nazionali che, a loro volta, possono proporre una pronuncia pregiudiziale sulla validità della decisione di adeguatezza[76]. Infatti, il potere di esecuzione che il RGPD[77] riconosce alla Commissione non le conferisce la competenza a limitare i poteri di cui dispongono le autorità di controllo[78].

A tal riguardo e come rilevato anche dall'Avvocato generale[79], l'autorità è tenuta a sospendere o a vietare un trasferimento di dati personali verso un Paese terzo qualora ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le clausole standard

---

maggio 2018, disponibile all'indirizzo internet: https://edpb.europa.eu/our-work-tools/our-documents/directrices/guidelines-22018-derogations-article-49-under-regulation_it.

[70] Linee guida EDPB, 2/2018 sulle deroghe di cui all'articolo 49 del regolamento 2016/679.

[71] Occorre rispettare il principio generale per cui le deroghe previste all'articolo 49 del RGPD non dovrebbero trasformarsi di fatto in una regola, essendo necessario limitarne l'applicazione a situazioni specifiche e purché ogni esportatore di dati garantisca che il trasferimento soddisfa un rigoroso test di proporzionalità e necessità.

[72] Il RGPD conferisce alle autorità di controllo poteri specifici, di cui all'articolo 58, paragrafo 2, lettera j).

[73] Adottata sulla base dell'articolo 45 RGPD.

[74] Ai sensi dell'articolo 77, paragrafo 1, RGPD.

[75] Si veda per analogia quanto stabilito per l'applicazione dell'articolo 28 della direttiva 95/46, Corte giust., 6 ottobre 2015, causa C-362/14, *Schrems I*, EU:C:2015:650, punto 47.

[76] Corte di giustizia, 16 luglio 2020, causa C-311/18, *Scherms II*, cit., punti 120 e 157.

[77] Ai sensi dell'articolo 46, paragrafo 2, lettera c), RGPD.

[78] Ai sensi dell'articolo 58, paragrafo 2, RGPD.

[79] Paragrafo 148 delle conclusioni dell'Avvocato generale.

di protezione dei dati non siano o non possano essere rispettate in tale Paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione non possa essere garantita con altri mezzi, ove l'esportatore dei dati stabilito nell'Unione non abbia egli stesso sospeso il trasferimento o messo fine a quest'ultimo.

6. Conclusioni

All'indomani della decisione della Corte, il ricorrente *Maximilian Schrems* ha continuato la sua azione legale in varie sedi giudiziarie e amministrative chiedendo di conoscere le basi giuridiche del trasferimento negli Stati Uniti dei dati raccolti da Facebook[80]. L'Autorità di controllo irlandese ha ordinato a Facebook di sospendere i trasferimenti dei dati verso gli Stati Uniti e di riprogettare il servizio. Se Facebook non rispetterà tale ingiunzione, il *DPC* irlandese ha il potere di multare la società fino al 4% del suo fatturato annuo. In attesa di un possibile terzo accordo Stati Uniti-Unione in materia[81], la valutazione del contesto giuridico del Paese di trasferimento spetterà "caso per caso" a ciascun esportatore sotto il controllo delle autorità con un eventuale rinvio, in caso di differenti posizioni, al Comitato europeo per la protezione dei dati. In particolare, l'esportatore dei dati (titolare o responsabile) dovrà esaminare se ci sia effettivamente bisogno dei servizi di un fornitore USA e quindi extra UE, rinegoziare eventuali clausole contrattuali, passare a un'altra base giuridica che legittimi il trattamento o cessare il trasferimento dei dati[82].

A tal proposito la sentenza ha una natura politica e può portare a ridisegnare i rapporti futuri tra operatori UE e statunitensi spingendo i primi a optare per fornitori europei in ragione del fatto che gli adempimenti necessari per trasferire i dati oltreoceano sembrano ormai troppo gravosi. Tale scelta rafforzerebbe il ruolo dell'Unione nella *digital economy*. D'altronde le Istituzioni europee auspicano un rafforzamento della competizione tecnologica europea che favorisca il Mercato unico dei dati[83]. Questi obiettivi possono essere raggiunti grazie a un adeguato apparato regolatorio[84] e tecnologico attento agli aspetti che garantiscono il rispetto dei diritti fondamentali.

In questo contesto si inserisce anche il progetto - di impulso tedesco e francese- "Gaia-X"[85] finalizzato a dar vita a un'infrastruttura di *cloud* europeo capace di rivaleggiare con i *big*

---

[80] L'associazione NOYB (l'associazione senza fini di lucro fondata dal Sig. Schrems nel 2017) ha presentato in totale 101 ricorsi davanti alle varie autorità garanti dell'UE, lamentando l'utilizzo, da parte di varie società i quali trasferiscono dati all'esterno dell'Unione senza una valida base giuridica "101 Complaints on EU-US transfers filed", 17 agosto 2020, disponibile all'indirizzo internet: https://noyb.eu/en/update-noybs-101-complaints-eu-us-data-transfers.

[81] Si veda Joint Press Statement from European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Wilbur Ross, 10 agosto 2020, disponibile all'indirizzo internet: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836.

[82] EDPB, risposte alle domande frequenti sulla sentenza della CGUE nella causa C-311/18 (Schrems II), 24 luglio 2020, disponibile all'indirizzo internet: https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_it.

[83] Comunicazione "*A digital single market for Europe*" del 6 maggio 2016; "*A European strategy for Data"* del 19 febbraio 2020, disponibile all'indirizzo internet: https://ec.europa.eu/digital-single-market/en.

[84] Si è in attesa auspicabilmente nel 2021 del "Digital Services Act" un nuovo pacchetto di normative sui servizi digitali che dovrebbe modernizzare l'attuale quadro giuridico, https://ec.europa.eu/commission/presscorner/detail/en/ip_20_962.

[85] Il progetto GAIA-X è consultabile *online*: https://www.data-infrastructure.eu/GAIAX/Navigation/EN/Home/home.html.

players statunitensi e aperta agli operatori europei che non vogliono ricorrere - anche alla luce della sentenza *Schrems II* - al mercato USA della *Big Tech* evitando così di trasferire i dati. All'indomani della decisione della Corte, la Commissione e gli Stati Uniti hanno annunciato in un comunicato stampa congiunto di avere iniziato le trattive per elaborare un quadro normativo migliorato adeguandosi alla sentenza della Corte di giustizia[86]. Tuttavia, nell'attesa di una nuova decisione sull'adeguatezza e dell'utilizzo da parte degli esportatori dei dati delle nuove clausole contrattuali standard[87] potrebbe verificarsi l'implementazione dell'offerta di servizi digitali basati in UE a favore del Mercato unico europeo.

[86] Comunicato della Commissione europea e degli Stati Uniti del 10 agosto 2020, disponibile all'indirizzo internet: https://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=684836.

[87] La Commissione ha pubblicato la revisione delle clausole contrattuali standard all'indirizzo internet: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries.