Dipartimento di Scienze Politiche

Cattedra di Diritto dell'Unione europea

Il trasferimento transfrontaliero dei dati personali: la tutela della privacy nell'Unione europea alla luce della sentenza *Schrems II*.

Prof. Francesco Cherubini

RELATORE

Maria Vittoria Mori
Matr. 088222

CANDIDATA

Anno Accademico 2020/2021

Indice

Abstract

Questo elaborato propone un'analisi della seconda sentenza *Schrems*, alla luce di quella che è stata la giurisprudenza europea sulla materia del trasferimento transfrontaliero dei dati. La sentenza *Schrems II* è considerata un secondo episodio della sentenza *Schrems I* e sono, per tale ragione, analizzate in un'ottica di continuità. Entrambe devono il nome al cittadino austriaco Maximilian Schrems, attivista per la privacy nell'Unione europea, coinvolto nella vicenda dei *transborder data flow*. Egli ha affermato ripetutamente, nel 2013 e successivamente nel 2015, che la legislazione statunitense non riconoscesse agli utenti del *social network* Facebook un livello di tutela dei dati personali equivalente a quello riconosciuto dalla normativa europea. Tuttavia, a partire dall'ultima sentenza del 16 luglio 2020, la prospettiva si è ampliata. Nonostante quest'ultima sentenza sia sorta da una controversia circa il trattamento dei dati personali dei cittadini dell'Unione europea trasferiti negli Stati Uniti, questa tematica si è intersecata con questioni che confluiscono in altri ambiti, quali le nuove frontiere del commercio dei dati e il concetto di *consumer*.

Considerazioni introduttive

Quando si fa riferimento alle sentenze *Schrems* si tratta il gruppo di sentenze che descrivono la posizione della giurisprudenza europea sulla materia del trasferimento transfrontaliero dei dati. Entrambe le sentenze prendono il nome dal cittadino austriaco, Maximilian Schrems. Egli, in molteplici sedi, ha affermato che la legislazione statunitense non riconoscesse agli interessati, ovvero agli utenti del *social network* Facebook, un livello di tutela dei dati personali equivalente a quello riconosciuto e proposto dalla normativa europea.

La prima sentenza *Schrems I*, fa riferimento alla pronuncia della Corte di giustizia dell'Unione europea in causa C-362/14, del 6 ottobre 2015, *Maximilian Schrems c. Data Protection Commissioner.* La seconda, in continuità con la prima come se ne fosse un "*second stage*"[1], fa riferimento alla pronuncia della Corte circa la causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems*. L'ultima sentenza del 16 luglio 2020 è fondamentale in quanto punto di cesura nell'interpretazione della protezione dei dati personali. Infatti, nonostante si parta da una controversia circa il trattamento dei dati personali dei cittadini europei nel territorio statunitense, le conseguenze hanno una portata che non è limitata agli accordi tra Unione europea e Stati Uniti d'America.

In quest'ottica, si nota ciò che Anu Bradford definisce il c.d. effetto Bruxelles, ovvero una globalizzazione normativa dell'Unione europea che, unilateralmente, esternalizza il diritto oltre i propri confini[2]. Il trasferimento transfrontaliero dei dati personali ne può essere un chiaro esempio.

Quella dell'Unione europea è sempre stata una "corsa verso l'alto"[3], alla ricerca di standard sempre più rigorosi degli ambienti normativi. Già nel 1995, con l'introduzione della direttiva 95/46/CE sulla protezione dei dati personali, l'Unione aveva optato per un approccio rigoroso *top-down*[4] della privacy dei cittadini. In tale direttiva la tematica base del diritto alla privacy era il c.d. *right to be let alone*[5], ovvero il diritto alla riservatezza. La regolamentazione successiva, fino all'attuale *General Data Protection Regulation* (GDPR), ha esteso questo effetto rendendolo globale. Tale estensione si nota soprattutto in rapporto ai precedenti accordi transatlantici, quali il *Safe Harbor Agreement* e il *Privacy Shield*. Infatti, già a partire dall'introduzione del GDPR, il trasferimento assume una portata generale nei confronti di Stati terzi

---

[1] S. FANTIN (2020: 5).

[2] A. BRADFORD (2020).

[3] Comunicazione della Commissione, del 10 maggio 2017, al Parlamento europeo e al Consiglio, COM(2017)240 def., *sulla gestione della globalizzazione.*

[4] Il modello *top-down* è una strategia di elaborazione e gestione delle informazioni che fa riferimento a un approccio generale del sistema ovvero se ne descrive in maniera generica e globale la finalità principale senza entrare nel merito dei dettagli e dei particolari.

[5] Il diritto alla privacy venne codificato per la prima volta da S. Warren e L. Brandeis in un articolo intitolato "The right to privacy", scritto per la rivista del dipartimento di giurisprudenza di Harvard (Harvard Law Review) il 15 dicembre 1890. Venne codificato proprio come diritto di essere lasciati da soli, o the right to be let alone.

che importano dati dall'Unione europea. In generale non si guarda più solo agli Stati Uniti.

Il nuovo GDPR si inserisce nella sentenza *Schrems II*, comportando una rilettura del contesto normativo tra la prima e la seconda sentenza. Lo stesso GDPR nei suoi primi considerando fa proprio riferimento al concetto di globalizzazione, ammettendo una necessità di trasferimento dei dati che sono sempre di più la manifestazione di un nuovo commercio, di una nuova rete di relazioni economiche. Tuttavia, la giurisprudenza europea, segnatamente alle sentenze concernenti gli avvenimenti che hanno coinvolto Facebook e Google, ha affermato come la tutela dei dati personali sia uno dei punti cardine dell'Unione europea. L'Unione ha cosi stabilito un primato della tutela sul commercio.

Infatti, è proprio in questo senso che le sentenze *Schrems* assumono un'importanza rilevante. Viene sostenuto in *Schrems I* e ribadito in *Schrems II* che, in caso di trasferimento dei dati all'estero, deve essere assicurata una continuità delle salvaguardie. Secondo quanto ricordato dalla Corte e dagli Avvocati generali di entrambe le sentenze, bisogna assicurare una continuità di protezione che si esplica oltre i confini dell'Unione europea. Tale continuità è indicata come "sostanziale equivalenza" e può essere assicurata anche attraverso dei mezzi diversi da quelli utilizzati dall'Unione. Tuttavia, l'equivalenza si deve riuscire a rintracciare nel risultato finale. Si dovrebbe trattare, nella sostanza, di un livello di tutela comparabile.

In questo senso, la sentenza *Schrems II* ha una portata di sistema, alla luce di come è stata ridisegnata la disciplina europea in merito al *transborder data flow*[6]. La tutela non riguarda solo i trasferimenti di dati tra imprese commerciali, ma tocca anche le condizioni e le salvaguardie in caso di accesso da parte delle autorità pubbliche nell'esercizio delle loro competenze in materia penale, di sicurezza o di *intelligence*. Quello che sostiene in maniera rinnovata la Corte è che non si può separare la sfera privata, intesta come commerciale, da quella pubblica, quindi l'ingerenza delle agenzie. Infatti, i dati costituiscono una fonte a cui attingono non solo operatori privati ma anche altre attività messe in atto da operatori pubblici, che hanno fini diversi da quelli commerciali. Il livello di tutela sostanzialmente equivalente in questo senso deve varcare anche la soglia pubblica, tutelando i dati dei cittadini, prima che dei consumatori, da interferenze che possano essere interpretate come eccessive.

In questo senso la sentenza *Schrems II* è espressione di una questione globale e ha portata sistemica. Infatti, questa problematica non è unicamente europea. Nel diritto dell'Unione europea, queste sentenze sono espressione di un movimento di convergenza del mondo della privacy, cioè di vari ordinamenti che adottano regolamenti in materia di privacy, che si basano su principi sostanziali affini o su simili meccanismi di *governance*, ad esempio l'istituzione di autorità garanti indipendenti. Si tratta di una tendenza globale che coinvolge molti Stati, tra cui la California, il Brasile, la Corea, l'Indonesia e il Giappone, con cui è stata creata una delle zone più ampie di scambio di dati

[6] C. KUNER (2012: 215).

per principi non identici ma comuni. Queste garanzie comuni possono assicurare la tutela dei dati e sono la *conditio sine qua non* posta dalla Corte di giustizia per assicurarne il trasferimento.

In questo senso, la privacy non è solo uno schema normativo. I dati e il loro trattamento hanno una rilevanza anche da un punto di vista più politico ed economico. La privacy viene intesa sempre di più come una delle linee di confine che definisce i sistemi democratici. In questo modo i cittadini degli Stati si distinguono, in base all'ordinamento e alle garanzie poste in capo a questi, in *data subject* e, in altri sistemi, come *consumers*. Assicurare che il trasferimento e l'accesso ai dati da parte di aziende private o autorità pubbliche rispettino i principi di proporzionalità e necessità[7]: sono queste le tematiche al centro della sentenza *Schrems II*, che vanno al di là della relazione transatlantica.

[7] Al considerando n. 152 del GDPR viene ricordato che "[l]e condizioni e le garanzie in questione possono comprendere procedure specifiche per l'esercizio di tali diritti da parte degli interessati, qualora ciò sia appropriato alla luce delle finalità previste dallo specifico trattamento, oltre a misure tecniche e organizzative intese a ridurre al minimo il trattamento dei dati personali conformemente ai principi di proporzionalità e di necessità".

Capitolo I

Regolamentazione, trattamento e trasferimento transfrontaliero dei dati: la giurisprudenza della Corte di giustizia

1.1 Il trasferimento transfrontaliero dei dati: sentenza *Schrems I*

Con l'espressione "sentenze *Schrems*" si intende il gruppo di sentenze della Corte di giustizia dell'Unione europea che hanno ad oggetto la materia della protezione dei dati personali. L'espressione accomuna le sentenze *Schrems I*[8] e *Schrems II*[9] in quanto identificano, in un rapporto di continuità, l'evoluzione della giurisprudenza della Corte nel trattare e tutelare i dati in territori terzi, laddove con terzi si intendono Stati non appartenenti all'Unione. Con l'esito della prima sentenza si segna infatti il passaggio dal *Safe Harbor Agreement*, un sistema di trasferimento transfrontaliero "primitivo", a un sistema apparentemente più tutelante, il *Privacy Shield*. La seconda sentenza invalida quest'ultimo, descrivendo una nuova tutela del cittadino e dei suoi dati all'interno dell'Unione europea e nel rapporto con terzi. *Schrems II* integra la materia della protezione con delle visioni innovative che si sono potenziate nel dibattito giurisprudenziale europeo. Appare quindi necessario ripercorrere le tappe delle normative che hanno condotto a quest'ultima sentenza.

La sentenza *Schrems I* si inserisce nello scenario della tutela dei dati personali, specificatamente, quelli soggetti a trasferimento transfrontaliero, cioè che vengono trasferiti e conservati in Stati non membri dell'Unione. Tale sentenza costituisce una parte determinante della materia, comportando una nuova stesura della regolamentazione europea sul trattamento dei dati. Comporta l'annullamento della decisione 2000/520/CE e la pronuncia circa l'interpretazione dell'art. 25, ai paragrafi 1 e 6, e dell'art. 28 della direttiva 95/46/CE. L'interpretazione risulta essere una chiara conseguenza della lettura del quadro normativo fornito dagli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea (Carta)[10].

Il trasferimento dei dati verso paesi terzi veniva formalmente garantito dalla decisione 2010/87/UE circa l'avvio delle clausole contrattuali tipo[11]. Tali clausole sono identificate come "garanzie sufficienti per la tutela della vita privata e dei diritti e della libertà fondamentali delle persone". Inoltre, lo stesso trasferimento risultava assicurato dal sistema c.d. "approdo sicuro"

---

[8] Sentenza della Corte di giustizia dell'Unione europea del 6 ottobre 2015, causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*.

[9] Sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems*.

[10] F. ACCARDO (2017: 155 ss.).

[11] Decisione della Commissione europea del 5 febbraio 2010, 2010/87, *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/CE del Parlamento europeo e del Consiglio*.

elaborato dallo *U.S. Department of Commerce* il 21 luglio 2000 e adottato dalla Commissione con decisione di adeguatezza 2000/520/CE[12]. Nel caso della sentenza *Schrems I*, i soggetti internazionali interessati sono l'Unione europea e gli Stati Uniti d'America. I dati venivano infatti sottoposti a trasferimento, per via della presenza di una sede della società americana Facebook Inc. in Irlanda.

Come rilevato dalle conclusioni dell'Avvocato generale Yves Bot del 23 settembre 2015, il problema sorse da specifiche rivelazioni portate alla luce da un cittadino austriaco, Maximilian Schrems. Egli dichiarò dinanzi all'Autorità garante dei dati personali dell'Irlanda che il diritto e la prassi statunitense fossero carenti circa la tutela dei dati personali di cittadini americani e non. Egli sostenne che non assicurassero un'adeguata tutela dei dati in sede di trasferimento. Tali contestazioni del cittadino austriaco interessavano la raccolta indifferenziata di dati e informazioni su larga scala, compiuta da programmi statunitensi connessi allo scandalo americano conosciuto come Datagate[13].

Nella fattispecie, lo scandalo emerse da un rapporto pubblicato da un informatico statunitense, Edward Snowden, in merito alle attività dei servizi di intelligence degli Stati Uniti e alle operazioni della *National Security Agency* (NSA). Tali divulgazioni avevano lo scopo di informare, cittadini e non, delle modalità del trattamento dei dati in suolo americano. Il Datagate viene ricondotto agli eventi successivi la pubblicazione della prima raccolta dei tabulati telefonici dei cittadini statunitensi da parte del *Guardian* e del *Washington Post*, in data 6 giugno 2013. A partire dal giorno successivo, il fenomeno di pubblicazione dilagò, coinvolgendo un programma americano c.d. PRISM. PRISM consisteva in un sistema operante in senso "duraturo e indiscriminato"[14] di controllo e di raccolta dei dati di cittadini residenti negli USA. Lo scandalo coinvolse aziende informatiche e *internet service providers* come Apple, Facebook, Google, Microsoft e Yahoo[15]. Una volta emersa la notizia si innescò un meccanismo di protesta volto a far cessare tali atti. Sebbene i provvedimenti contro le aziende tardarono ad arrivare, le proteste di attivisti privati, preoccupati per le violazioni della propria privacy, perdurarono. In Europa, condivise questa rimostranza Maximilian Schrems.

La scoperta dell'operazione di sorveglianza del programma PRISM ha "gettato un'ombra sul rispetto delle norme del diritto dell'Unione in occasione dei trasferimenti di dati personali verso [le] imprese stabilite negli Stati

---

[12] F. ACCARDO (2017: 155 ss.).

[13] Con il c.d. Datagate si indicano una serie di divulgazioni sulle operazioni di sorveglianza di massa nei confronti dei cittadini statunitensi e stranieri compiute dalla National Security Agency a partire dal 2001. Tali attività sono perdurate fino al 2011. Si individua la fine del fenomeno solamente successivamente all'approvazione, da parte del Senato americano, del Freedom Act, il 2 giugno 2015.

[14] M. NINO (2013: 727 ss.).

[15] Comunicazione della Commissione, del 27 novembre 2013, al Parlamento europeo e al Consiglio, COM(2013)846 e COM(2013)847 def., *sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite.*

Uniti"[16]. Si può quindi dedurre che le dichiarazioni di Snowden furono alla base delle richieste di Schrems sulla tutela dei propri dati, in sede di trasferimento transfrontaliero. Venne così messa in luce l'inefficacia del sistema precedentemente vigente, c.d. *Safe Harbor Agreement*, evidenziandone i limiti e reclamando un'evoluzione della tutela dei dati personali.

Il trasferimento in questione si definisce transatlantico e unidirezionale, in quanto lo spostamento dei dati procede univocamente dall'Unione europea verso gli Stati Uniti d'America. Inoltre, siffatto trasferimento viene messo in risalto da una discrasia tra l'operato delle istituzioni europee e la materia americana. Le prime si occupano di tutela e di sicurezza dei dati dei propri cittadini[17], mentre la prassi statunitense è diretta verso un aspetto più commerciale circa il trattamento dei dati[18]. Difatti, il ricordato accordo di "approdo sicuro" aspirava proprio ad "agevolare i rapporti commerciali tra USA e UE, [prevedendo] l'adesione volontaria di organizzazioni americane operanti in Europa ad alcuni principi europei in materia di dati personali"[19].

In tale contesto si inserì la sentenza *Maximilian Schrems c. Data Protection Commissioner*, in causa C-362/14. La stessa aveva a oggetto una domanda di pronuncia in via pregiudiziale[20], conformemente all'art. 267 del Trattato sul funzionamento dell'Unione europea (ex art. 234 TCE). Questa venne proposta alla Corte di giustizia dell'Unione europea, dalla Corte d'appello irlandese, in seno alla controversia sorta fra Maximilian Schrems e il *Commissioner*. La domanda sorse per il rifiuto del *Commissioner* di istituire una denuncia da parte di Schrems contro la società americana Facebook Inc., la cui sede europea si colloca in Irlanda. Tale società gestisce il social network Facebook al quale Schrems era iscritto dal 2008. La motivazione alla base della sollecitazione fu di opporsi alla prassi statunitense della raccolta e conservazione dei dati, la quale si scontrava con la disciplina europea.

In tale causa vennero affrontate due questioni fondamentali per l'evoluzione della protezione dei dati nell'Unione. La prima fu la pronuncia circa l'interpretazione sull'art. 25, paragrafi 1 e 6, e sull'art. 28 della direttiva

---

[16] Conclusioni dell'Avvocato generale Yves Bot del 23 settembre 2015, causa C-362/2014, *Maximilian Schrems c. Data Protection Commissioner [Ireland]*.

[17] Si possono ricordare in merito due organi dell'Unione europea quali: il Garante europeo della protezione dei dati (GEPD) e il Comitato europeo per la protezione dei dati (EDPB). Quest'ultimo istituito a partire dal 2018, con il compito di garantire la corretta applicazione del Regolamento generale sulla protezione dei dati (RGPD) e della direttiva sull'applicazione della legge sulla protezione dei dati.

[18] R. F. JØRGENSEN, T. DESAI (2017: 106 ss.).

[19] A. GIATTINI (2016: 247).

[20] L'art. 267 TFUE (ex art. 234 TCE) consolida la competenza della Corte di giustizia dell'Unione europea a pronunciarsi in via pregiudiziale nelle materie riportate dallo stesso articolo: a) sull'interpretazione dei trattati; b) sulla validità e l'interpretazione degli atti compiuti dalle istituzioni, dagli organi o dagli organismi dell'Unione. Con particolare riferimento al punto b) dello stesso articolo citato, per la sentenza Schrems risulta fondamentale la fattispecie seguente: "[q]uando una questione del genere è sollevata dinanzi ad un organo giurisdizionale di uno degli Stati membri, tale organo giurisdizionale può, qualora reputi necessaria per emanare la sua sentenza una decisione su questo punto, domandare alla Corte di pronunciarsi sulla questione".

europea 95/46/CE. E inoltre, la pronuncia circa la validità della decisione 2000/520/CE, presa sulla base dell'art. 25 di cui sopra.

Nella sostanza, Schrems sosteneva che il *Safe Harbor Agreement* non fosse in grado di assicurare una protezione effettiva dei propri dati, una volta raccolti da Facebook e trasferiti negli Stati Uniti. In sentenza, difatti, la specifica della Corte di giustizia recita:

> "[c]hiunque risieda nel territorio dell'Unione e desideri utilizzare Facebook è tenuto, al momento della sua iscrizione, a sottoscrivere un contratto con Facebook Ireland, una controllata di Facebook Inc., situata, da parte sua, negli Stati Uniti. I dati personali degli utenti di Facebook residenti nel territorio dell'Unione vengono trasferiti, in tutto o in parte, su server di Facebook Inc. ubicati nel territorio degli Stati Uniti, ove essi sono oggetto di un trattamento"[21].

Maximilian Schrems provò ad appellarsi, inizialmente, al commissario dell'Autorità garante dei dati personali dell'Irlanda, chiedendo che venissero esercitate le competenze statutarie e che fosse vietato a Facebook Ireland di trasferire e conservare i dati nella sede statunitense. Ritenendo che non esistessero prove che i dati personali di Schrems fossero pervenuti alla NSA, il commissario respinse la denuncia in quanto "priva di fondamento"[22]. Ricordando poi che

> "[…] le censure formulate dal sig. Schrems nella sua denuncia non potevano essere fatte valere in maniera utile, in quanto ogni questione relativa all'adeguatezza della protezione dei dati personali negli Stati Uniti doveva essere risolta in conformità alla decisione 2000/520 e che, in tale decisione, la Commissione aveva constatato che gli Stati Uniti d'America assicuravano un livello di protezione adeguato"[23].

Conseguentemente, Schrems avanzò un ricorso dinanzi alla Corte d'appello irlandese, contro il respingimento del suo appello al commissario. Il giudice della Corte, tuttavia, chiarì che "la sorveglianza elettronica e l'intercettazione dei dati personali trasferiti dall'Unione verso gli Stati Uniti rispondevano a finalità necessarie e indispensabili per l'interesse pubblico"[24]. Stabilì, in un primo momento, l'effettiva validità e sicurezza del *Safe Harbor Agreement* e respinse il ricorso di Schrems. Eppure, le prassi di sorveglianza e intercettazione americana suscitarono l'interesse dello stesso giudice, che le qualificò come "eccessi considerevoli". Sottolineò, inoltre, come tali "eccessi" contrastassero con il diritto interno irlandese, il quale

> "[…] vieta il trasferimento dei dati personali al di fuori del territorio nazionale, fatti salvi i casi in cui il paese terzo in questione assicura un livello di protezione adeguato della vita privata, nonché dei diritti e delle libertà fondamentali"[25].

---

[21] Sentenza della Corte di giustizia *Schrems I*, punto 27.
[22] Ivi, punto 29.
[23] *Ibidem*.
[24] Ivi, punto 30.
[25] Ivi, punto 32.

Di fatto, tale accesso indifferenziato appariva antitetico rispetto alla tutela garantita dal principio di proporzionalità della Costituzione irlandese. Pertanto, conformemente al diritto interno, sarebbe stato necessario che le intercettazioni e il trattamento dei dati fossero stati mirati e giustificati nell'ottica di tutelare la sicurezza nazionale e di reprimere la criminalità[26]. In materia di trasferimento transfrontaliero, si può dedurre che il diritto irlandese si pone inflessibilmente a favore di una rigida tutela della privacy del cittadino. In questo senso si rivelò la discrasia tra il trattamento dei dati nei due Paesi: l'Irlanda e gli Stati Uniti. Infatti, ponendo che il procedimento principale si fosse dovuto definire sulla base del solo diritto interno irlandese, questo avrebbe definito la prassi americana come illecita. In seno alla Corte irlandese, questo mancato coordinamento destò

> "[…] un serio dubbio sul fatto che gli Stati Uniti d'America assicurino un livello di protezione adeguato dei dati personali, il commissario avrebbe dovuto compiere un'indagine sui fatti lamentati dal sig. Schrems nella sua denuncia e il commissario ha erroneamente respinto quest'ultima"[27].

Ai sensi dell'art. 51 della Carta dei diritti fondamentali dell'Unione europea, la Corte d'appello irlandese osservò che la causa sollevata da Maximilian Schrems interessava anche l'attuazione del diritto dell'Unione. Ne risultò che "la legittimità della decisione di cui al procedimento principale [doveva] essere valutata sulla scorta del diritto dell'Unione"[28]. Pertanto, conformemente all'art. 267 TFUE, la Corte d'appello decise di sospendere il procedimento e di sottoporre alla Corte di giustizia la domanda di pronuncia pregiudiziale circa due questioni principali:

> "1) [s]e, nel decidere in merito a una denuncia presentata a un'autorità indipendente investita per legge delle funzioni di gestione e di applicazione della legislazione sulla protezione dei dati, secondo cui i dati personali sono trasferiti a un paese terzo (nel caso di specie, gli Stati Uniti d'America) il cui diritto e la cui prassi si sostiene non prevedano adeguate tutele per i soggetti interessati, tale autorità sia assolutamente vincolata dalla constatazione in senso contrario dell'Unione contenuta nella decisione 2000/520, tenuto conto degli articoli 7, 8 e 47 della Carta, nonostante le disposizioni dell'articolo 25, paragrafo 6, della direttiva 95/46.
> 2) Oppure, in alternativa, se detta autorità possa e/o debba condurre una propria indagine sulla questione alla luce degli sviluppi verificatisi nel frattempo, successivamente alla prima pubblicazione della decisione 2000/520"[29].

---

[26] Il *Data Protection (Amendment) Act 2003* stabilisce che "the data shall have been obtained only for one or more specified, explicit and legitimate purposes, shall not be further processed in a manner incompatible with that purpose or those purposes, shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they were collected or are further processed, and shall not be kept for longer than is necessary for that purpose or those purposes".
[27] Sentenza della Corte di giustizia *Schrems I*, punto 33.
[28] Ivi, punto 34.
[29] Ivi, punto 36.

La prima questione verteva sull'interpretazione dell'art. 25, paragrafi 1 e 6, e sull'art. 28 della direttiva 95/46. Circa il trasferimento dei dati personali verso paesi terzi, l'art. 25, par. 1, afferma che

> "[gli] Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva"[30].

Riconoscendo, al considerando n. 56, che i trasferimenti di dati personali dagli Stati membri verso paesi terzi fossero necessari allo sviluppo degli scambi internazionali, l'art. 25, par. 1 della direttiva poneva come principio che tali trasferimenti potessero avere luogo esclusivamente se i paesi terzi avessero garantito un livello di protezione adeguato. Riguardo l'art. 25, al par. 6 si ribadisce che:

> "[l]a Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2 [della direttiva 95/46/CE], che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona"[31].

Ai sensi dell'art. 28 della stessa direttiva, si ricordava essere presente un c.d. criterio di adeguatezza delle norme che tutelano i dati personali. Stando a tale criterio, in caso non si fosse accertato un livello di tutela adeguato, si sarebbe dovuto disporre un intervento delle autorità di controllo, a garanzia di una tutela effettiva dei dati trasferiti. Il ruolo di tali autorità di controllo veniva disciplinato ai paragrafi 1, 2, 3 e 6 dell'art. 28:

> "1. [o]gni Stato membro dispone che una o più autorità pubbliche siano incaricate di sorvegliare, nel suo territorio, l' applicazione delle disposizioni di attuazione della presente direttiva, adottate dagli Stati membri. Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite.
> 2. Ciascuno Stato membro dispone che le autorità di controllo siano consultate al momento dell'elaborazipne delle misure regolamentari o amministrative relative alla tutela dei diritti e delle libertà della persona con riguardo al trattamento dei dati personali.
> 3. Ogni autorità di controllo dispone in particolare:
> – di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
> – di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, conformemente all'articolo 20, e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento,

[30] Direttiva (CE) del Parlamento europeo e del Consiglio, del 24 ottobre 1995, 95/46, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.
[31] *Ibidem*.

> ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali; – del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva ovvero di adire per dette violazioni le autorità giudiziarie.
> […] 6. Ciascuna autorità di controllo, indipendentemente dalla legge nazionale applicabile al trattamento in questione, è competente per esercitare , nel territorio del suo Stato membro, i poteri attribuitile a norma del paragrafo 3. Ciascuna autorità può essere invitata ad esercitare i suoi poteri su domanda dell'autorità di un altro Stato membro […]"[32].

Da quanto emerge dagli articoli precedenti, si può affermare che le autorità di controllo avessero il compito di trovare un "giusto equilibrio fra da un lato, il rispetto del diritto fondamentale alla vita privata e, dall'altro, gli interessi che impongono una libera circolazione dei dati personali"[33]. Motivo per cui "dette autorità [disponevano] di un'ampia gamma di poteri e questi, elencati in maniera non esaustiva all'art. 28, par. 3, della direttiva 95/46, costituiscono altrettanti mezzi necessari all'adempimento dei loro compiti"[34].

Pertanto, si decretò come gli articoli 25 e 28 imponessero delle garanzie al trasferimento dei dati verso paesi terzi. L'art. 25 stabilì di accertare che un paese terzo garantisse un livello adeguato di protezione dei dati personali che verso tale paese fossero trasferiti. L'art. 28 definì i poteri dei garanti nazionali. La Corte di giustizia, infatti, venne chiamata a precisare se, in presenza di una siffatta disposizione, "[l']autorità nazionale di controllo [potesse] esaminare il ricorso di un cittadino dell'Unione, che [contestasse] la violazione dei propri dati trasferiti verso il paese terzo interessato dalla decisione"[35]. Inoltre, al considerando n. 57 della direttiva 95/46, si chiarì in definitiva che i trasferimenti di dati personali verso paesi terzi che non offrissero un livello di protezione adeguato dovessero essere vietati. Pertanto,

> "[i]n virtù delle considerazioni che precedono, si deve rispondere alle questioni sollevate che l'articolo 25, paragrafo 6, della direttiva 95/46, letto alla luce degli articoli 7, 8 e 47 della Carta, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, quale la decisione 2000/520, con la quale la Commissione constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, esamini la domanda di una persona relativa alla protezione dei suoi diritti e libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato"[36].

Nondimeno, il secondo interrogativo pregiudiziale sottoposto alla Corte di giustizia interessò la fondatezza della decisione 2000/520/CE. Suddetta decisione venne adottata dalla Commissione sulla base dell'art. 25, par. 6, della

[32] Direttiva 95/45.
[33] Sentenza della Corte di giustizia *Schrems I*, punto 42.
[34] Ivi, punto 43.
[35] A. GIATTINI (2016: 248 ss.).
[36] Sentenza della Corte di giustizia *Schrems I*, punto 66.

direttiva 95/46. Circa la validità della decisione, la Corte si focalizzò sull'adeguatezza del livello di protezione dei dati personali dei cittadini dell'UE trasferiti negli Stati Uniti e sulla carenza di mezzi che consentissero ricorsi giurisdizionali a disposizione dei cittadini dell'UE che lamentassero violazioni dei propri dati personali[37].

La questione centrale interessò proprio il termine "adeguatezza". Venne stabilito che il termine "adeguato" non figurasse come un "livello di protezione […] «identico» a quello richiesto nell'Unione"[38], ma che questo dovesse comunque identificare un paese che "assicuri effettivamente un livello di protezione delle libertà e dei diritti fondamentali sostanzialmente equivalente a quello garantito dall'Unione in forza della direttiva 95/46"[39].

Altrimenti, sarebbe stato disatteso l'esplicito obbligo di protezione dei dati personali di cui all'art. 8, par. 1, della Carta[40]. In questo senso, si accostò il termine "adeguato" al suo corrispettivo di "sostanzialmente equivalente", così che, in conformità dell'art. 25 della direttiva, la Commissione fosse tenuta a valutare "tutte le circostanze relative ad un trasferimento dei dati personali verso un paese terzo"[41].

Si può concludere che, come dichiarato dalla Corte di giustizia riunitasi in Grande Sezione[42],

> "1) [l']articolo 25, paragrafo 6, della direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, come modificata dal regolamento (CE) n. 1882/2003 del Parlamento europeo e del Consiglio, del 29 settembre 2003, letto alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea, deve essere interpretato nel senso che una decisione adottata in forza di tale disposizione, come la decisione 2000/520/CE della Commissione, del 26 luglio 2000, a norma della direttiva 95/46 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, con la quale la Commissione europea constata che un paese terzo garantisce un livello di protezione adeguato, non osta a che un'autorità di controllo di uno Stato membro, ai sensi dell'articolo 28 di tale direttiva, come modificata, esamini la domanda di una persona relativa alla protezione dei suoi diritti e delle sue libertà con riguardo al trattamento di dati personali che la riguardano, i quali sono stati trasferiti da uno Stato membro verso tale paese terzo, qualora tale persona faccia valere che il diritto e la prassi in vigore in quest'ultimo non garantiscono un livello di protezione adeguato.

---

[37] S. CRESPI (2016: 687 ss.); A. GIATTINI (2016: 247 ss.).

[38] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe del 19 dicembre 2019, causa C-311/2018, *Data Protection Commissioner contro Facebook Ireland Limited, Maximillian Schrems*.

[39] Conclusioni dell'Avvocato generale Bot *Schrems I*, punto 141.

[40] Ivi, punto 148.

[41] A. GIATTINI (2016: 249).

[42] La Corte può riunirsi in seduta plenaria, in grande sezione (quindici giudici) o in sezioni composte da cinque o tre giudici. Essa si riunisce in grande sezione quando lo richiede uno Stato membro o un'istituzione parte della causa, nonché per trattare cause particolarmente complesse o importanti.

2) La decisione 2000/520 è invalida"[43].

In generale, la decisione 2000/520 su cui si fondava il *Safe Harbor Agreement* doveva rispettare la tutela della vita privata e della vita familiare, di cui all'art. 7 della Carta, e dei dati personali, di cui all'art. 8 della stessa, consacrati come diritti fondamentali dalla giurisprudenza della Corte[44]. Questi sembrerebbero "svuotati di significato" qualora la regolamentazione consentisse un accesso ingiustificato, casuale e generalizzato, senza basi di ispezione. Le basi dovrebbero essere dovute ai "motivi di sicurezza nazionale o di prevenzione della criminalità", con la necessità "che tali pratiche fossero accompagnate da garanzie adeguate e verificabili"[45].

Pertanto, Schrems sembrerebbe aver contestato il sistema di approdo sicuro che venne istituito dalla decisione 2000/520/CE. In particolare, la sollecitudine in questo caso interessò gli Stati Uniti d'America, coinvolgendo successivamente i paesi terzi su cui tale sistema di approdo esplicava la propria efficacia giuridica, stando alla decisione 2010/87/UE. Ai sensi dell'art. 267 TFUE e alla luce dei citati articoli 7 e 8 della Carta, la Corte di giustizia si è espressa in via pregiudiziale sulle obiezioni mosse dal cittadino austriaco Schrems nei confronti del regime di approdo sicuro[46]. Pertanto, sebbene Schrems non contestò formalmente la validità né della direttiva 95/46 né della decisione 2000/520, bensì la prassi statunitense, le conseguenze si estesero al *Safe Harbor Agreement*. Quest'ultimo venne sostituito da un nuovo accordo tra l'Unione europea e gli Stati Uniti.

Riconducendosi alle conclusioni dell'Avvocato generale Bot, si può sostenere come suddetta decisione dovesse consentire il flusso di dati tra l'Unione europea e gli Stati Uniti. Questa tuttavia avrebbe dovuto disporre una protezione dei dati dei cittadini adeguata, "[così] come richiesto dal diritto dell'Unione". È in questa direzione che la giurisprudenza europea progredisce, grazie alla sentenza *Schrems I* e all'approdo ad altri sistemi di tutela dei dati più evoluti e conformi all'evoluzione della materia. Una prima tappa è segnata dall'*EU-US Privacy Shield*[47] e dall'approdo al *General Data Protection Regulation*[48].

1.2 Dal *Safe Harbor Agreement* allo *EU-US Privacy Shield*

[43] Sentenza della Corte di giustizia *Schrems I*.
[44] Sentenza della Corte di giustizia del 13 maggio 2014, causa C-131/12, *sul diritto all'oblio, Google Spain e Google*.
[45] Sentenza della Corte di giustizia *Schrems I*, punto 34.
[46] H. HOFFMAN (2015).
[47] Decisione di esecuzione (UE) della Commissione del 16 luglio 2016, 2016/1250, *sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy*.
[48] Regolamento (UE) del Parlamento europeo e del Consiglio, del 27 aprile 2016, 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*.

La sentenza *Schrems I* ha costituito la premessa di una modifica sostanziale della regolamentazione del trasferimento transfrontaliero dei dati. Di coerenza, la materia ha dovuto sottoporsi a un disciplinamento adeguato, volto a non incorrere in problemi di analoga fattispecie. Il sistema di controllo e di regolamentazione si è evoluto in questo senso, con quello che ricordiamo come lo scudo UE-USA per la privacy o *EU-US Privacy Shield*.

Il regime dell'approdo sicuro o *Safe Harbor Agreement* era un accordo commerciale tra l'Unione europea e gli Stati Uniti d'America fondato sul trasferimento dei dati personali[49]. Il principio si fondava sulla decisione 2000/520/CE della Commissione, del 26 luglio 2000 e, perciò, sulla direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. I quesiti pregiudiziali sottoposti alla Corte di giustizia riesaminavano l'art. 25, par. 6, e l'art. 28 della direttiva 95/46/CE e, integralmente, la validità della decisione 2000/520/CE. Il 6 ottobre 2015, la Corte di giustizia invalidò la decisione 2000/520/CE.

Invalidata la decisione, fu necessario reintegrare un regolamento che adottasse misure confacenti e appropriate per il trasferimento verso gli Stati Uniti, entro i termini dell'Unione[50]. Già nel 2013 infatti, la Commissione europea, nelle comunicazioni 846[51] e 847[52], confermò l'esistenza del sistema di sorveglianza americano e, di conseguenza, la necessità di ristabilire un clima di fiducia nei rapporti tra gli Stati Uniti e l'Unione europea. In quest'ottica, si manifestò la necessità di ripristinare il rapporto commerciale fondato sui dati, fondato su forti misure di salvaguardia.

È qui che si inserì lo scudo UE-USA per la privacy o *EU-US Privacy Shield*[53]. Il 12 luglio 2016 il *Privacy Shield* venne introdotto con la decisione di esecuzione 2016/1250/UE della Commissione europea. Tale decisione risultava a norma dell'adeguatezza della protezione offerta dagli Stati Uniti, stabilita nella direttiva 95/46, non modificata né invalidata dalla precedente controversia in sentenza *Schrems I.* Il nuovo accordo sembrava adempiere e rispettare le norme istituite dal TFUE, dalla direttiva 95/46/CE del Parlamento europeo e del Consiglio, in particolar modo del suo art. 25, par. 6. Questo venne confermato dal Garante europeo della protezione dei dati nel parere 4/2016 relativo al progetto di decisione sull'adeguatezza del regime del *Privacy Shield*, del 30 maggio 2016[54].

---

[49] A. GIATTINI (2016: 247 ss.).

[50] Comunicazione della Commissione, del 27 novembre 2013, al Parlamento europeo e al Consiglio, COM(2013)846 def., *sul ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*.

[51] *Ibidem*.

[52] Comunicazione della Commissione *sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*.

[53] Comunicazione della Commissione, del 29 febbraio 2016, al Parlamento europeo e al Consiglio, COM(2016)117 fin., *Trasferimenti transatlantici di dati – Ripristinare la fiducia attraverso solide garanzie*.

[54] Parere del Garante europeo della protezione dati del 30 maggio 2016, 4/2016, *relativo al progetto di decisione sull'adeguatezza del regime dello scudo UE-USA per la privacy*.

Successivamente alla sentenza *Schrems I*, la Corte rilevò che la Commissione sostenne che il sistema americano, nella legislazione nazionale o negli accordi internazionali, non garantisse un livello di protezione adeguato[55]. Circa l'adeguatezza, al punto 10 della decisione 2016/1250 è ricordato che "l'espressione «livello di protezione adeguato» […] esige che il paese terzo assicuri un livello di protezione delle libertà e dei diritti fondamentali «sostanzialmente equivalente»" a quello che viene garantito all'interno dell'Unione, in forza della direttiva 95/46/CE, letta alla luce della Carta dei diritti fondamentali. Anche se gli strumenti di cui tale paese terzo si avvale possono essere diversi da quelli stabiliti all'interno dell'Unione, tali devono comunque rivelarsi efficaci nella prassi[56]. La Corte di Lussemburgo non mancò di sottolineare che, nella prassi statunitense, non fossero presenti normative adeguate a garantire una tutela efficace o a limitare eventuali ingerenze da parte delle agenzie americane. Infatti, sembrerebbe che gli Stati Uniti fossero autorizzati – a discrezione del caso – a compiere ingerenze laddove perseguissero obiettivi legittimi, come la sicurezza nazionale[57].

Il funzionamento del nuovo sistema si fondava, piuttosto, su una base sostanzialmente volontaria, ossia su un sistema di autocertificazione. L'organizzazione statunitense si sarebbe dovuta impegnare a rispettare i principi sulla privacy che venivano stabiliti dal *Privacy Shield* e i c.d. "principi supplementari", pubblicati dallo *U.S. Department of Commerce*. Il *Privacy Shield* si applicava integralmente sia ai titolari sia ai procuratori, o responsabili del trattamento. Inoltre, si specificava come "un contratto [dovesse] vincolare il responsabile del trattamento ad agire esclusivamente secondo le istruzioni del titolare del trattamento dell'UE" e "a prestargli assistenza per rispondere alle persone che esercitano i loro diritti nell'ambito dei principi"[58].

In tale contesto è bene ricordare che, successivamente al crollo del *Safe Harbor Agreement* sancito dalla causa *Schrems I*, la direttiva 95/46/CE rimase ancora in vigore e continuò a definire gli accordi presi in materia, tra cui lo stesso *Privacy Shield*. Infatti,

> "[f]ermo restando il rispetto delle disposizioni nazionali adottate in applicazione della direttiva 95/46/CE, la presente decisione ha l'effetto di autorizzare il trasferimento dei dati personali dai titolari o responsabili del trattamento nell'Unione alle organizzazioni presenti negli USA che si sono autocertificate come aderenti ai principi presso il Dipartimento del Commercio e si sono impegnate a conformarsi agli stessi. I principi si applicano al trattamento dei dati personali da parte di organizzazioni statunitensi esclusivamente se il trattamento da parte dell'organizzazione esula dall'ambito di applicazione della normativa dell'Unione. Lo scudo lascia impregiudicata l'applicazione della

[55] Sentenza della Corte di Giustizia *Schrems I,* punto 97.
[56] Ivi*,* punti 73 e 74.
[57] Ivi, punti 88 e 89.
[58] Decisione di esecuzione della Commissione del 12 luglio 2016, 2016/1250, *sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy*.

> normativa dell'Unione che disciplina il trattamento dei dati personali negli Stati membri"[59].

Successivamente al *Privacy Shield*, si profilarono delle reazioni contrarie, tra cui si ricordano quelle degli europarlamentari Jan Philipp Albrecht, Judith Sargentini e Guy Verhofstadt e dello stesso Maximilian Schrems. Quest'ultimo:

> "[…] ha pubblicato due libri riguardo alla sua azione contro le presunte violazioni della protezione dei dati, ha tenuto conferenze, alcune delle quali retribuite, in particolare presso organizzatori professionali, ha registrato numerosi siti internet quali blog, petizioni on line e siti di campagne di raccolta fondi per i procedi-menti contro la resistente nel procedimento principale. Egli ha fondato, inoltre, un'associazione intesa a far rispettare il diritto fondamentale alla protezione dei dati, ha ricevuto diversi premi e ha ottenuto la cessione, da parte di oltre 25 000 persone in tutto il mondo, dei loro diritti al fine di far valere tali diritti nella presente causa"[60].

In linea con quelle che furono le richieste portate avanti con la prima sentenza *Schrems*, molti cittadini e parlamentari chiesero lo sviluppo di un meccanismo implementato di ricorso. Ovvero che i singoli cittadini dell'Unione europea potessero godere di un sistema più trasparente e di una giurisprudenza che consentisse di ricorrere contro le agenzie di *intelligence* americane[61]. Si ritenne che, nonostante il *Privacy Shield* offrisse dei perfezionamenti sul sistema di approdo dei dati, non fosse comunque risolutivo di problemi fondamentali che vennero rintracciati "on both the commercial aspects and the access by public authorities to data transferred under the Privacy Shield"[62]. Inoltre, il Garante europeo della protezione dei dati Giovanni Buttarelli, emanò una considerazione il 30 maggio 2016, nella quale affermò che "[il] Privacy Shield, come proposto, non [fosse] abbastanza robusto da resistere a un futuro esame minuzioso della Corte [UE]"[63]. Alla luce della giurisprudenza europea, sembrava necessario che la materia venisse regolamentata solidamente, senza lasciare spazio a vuoti normativi. Infatti, è fondamentale ricordare che la materia qui disciplinata assume un rilievo sempre maggiore. I trasferimenti internazionali dei dati sono oggi imprescindibili per l'economia mondiale e per tutti i servizi di cui usufruiamo quotidianamente.

Il 16 luglio 2020, la decisione di esecuzione 2016/1250/UE della Commissione sull'adeguatezza della protezione offerta dal *Privacy Shield*, venne

---

[59] Decisione di esecuzione della Commissione del 12 luglio 2016, 2016/1250, *sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy*.
[60] Sentenza della Corte di giustizia dell'Unione europea del 25 gennaio 2018, causa C-498/16, *Maximilian Schrems c. Facebook Ireland Limited*, punto 12.
[61] Risoluzione del Parlamento europeo del 17 maggio 2016, 2016/2727(RSP), *sui trasferimenti transatlantici di dati*.
[62] Statement of the article 29 Working Party, 13 April 2016, *on the opinion on the EU-U.S. Privacy Shield*.
[63] Considerazione del Garante europeo della protezione dei dati del 30 maggio 2016, EDPS/2016/11, *Privacy Shield: more robust and sustainable solution needed*.

dichiarata invalida dalla Corte di giustizia dell'Unione europea con la sentenza *Schrems II*, nella causa 311/18[64].

1.3 L'approdo al General Data Protection Regulation: il Regolamento europeo 2016/679

Come è stato ricordato nei paragrafi precedenti, lo zoccolo duro della regolamentazione e del trattamento dei dati nell'Unione europea e in spostamenti transfrontalieri, è costituito dalla direttiva 95/46/CE, in vigore per tutta la trattazione di cui sopra. Coerentemente, si può affermare che tale direttiva costituisse anche il perno dei problemi circa la materia dei dati e della loro disciplina in paesi terzi. La direttiva rimase in vigore fino al subentro del *General Data Protection Regulation* (GDPR), il nuovo regolamento europeo sulla protezione dei dati (REPD).

Il progetto del GDPR risale al 25 gennaio 2012, quando la Commissione europea presentò la proposta di regolamento al Parlamento europeo e al Consiglio europeo. Nella primavera dell'anno successivo, il Parlamento approvò il regolamento. Successivamente alla co-decisione degli organi europei (Parlamento, Commissione e Consiglio europeo) avvenuta il 24 giugno 2015, il regolamento venne pubblicato nella Gazzetta Ufficiale dell'Unione europea (GUUE). L'entrata in vigore fu successiva a una fase di implementazione della durata due anni. Come ricordato dall'art. 99, par. 2, del regolamento, dal 25 maggio 2018 il GDPR entrò in vigore esplicando la propria efficacia giuridica in tutti i Paesi dell'Unione europea. Il regolamento è tutt'ora in vigore e la sua rilevanza nel contesto normativo europeo nel trattamento dei dati è stata ribadita nuovamente dalla sentenza *Schrems II*.

Il regolamento 2016/679/UE del Parlamento europeo e del Consiglio, del 27 aprile 2016, interessa la protezione delle persone fisiche con riguardo al trattamento dei dati personali e alla libera circolazione di questi ultimi. Come precedentemente anticipato, stando all'art. 94, l'entrata in vigore del GDPR comporta che "la direttiva 95/46/CE è abrogata a decorrere da 25 maggio 2018"[65], data di entrata in vigore dello stesso Regolamento (art. 99, par. 2). E che

> "[i] riferimenti alla direttiva abrogata si intendono fatti al presente regolamento. I riferimenti al gruppo per la tutela delle persone con riguardo al trattamento dei dati personali istituito dall'articolo 29 della direttiva 95/46/CE si intendono fatti al comitato europeo per la protezione dei dati istituito dal presente regolamento"[66].

Gli altri accordi, come ricordato dall'art. 96 dello stesso GDPR, "restano in vigore [se] conclusi dagli Stati membri prima [del] 24 maggio 2016 e conformi al diritto dell'Unione [europea] applicabile prima di tale data".

---

[64] Sentenza della Corte di giustizia *Schrems II*.
[65] Regolamento (UE) 2016/679.
[66] *Ibidem*.

Alla base del GDPR si collocano, al considerando n. 1, l'art. 8, par. 1, della Carta dei diritti fondamentali dell'Unione europea e l'art. 16, par. 1, del Trattato sul funzionamento dell'Unione europea. Questi pongono il trattamento dei dati di carattere personale come diritto fondamentale, pur essendosi la Corte già espressa a favore di questa elocuzione[67]. Lo stesso art. 16 TFUE "conferisce al Parlamento europeo e al Consiglio il mandato di stabilire le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale e le norme relative alla libera circolazione di tali dati"[68], come ricordato al considerando n. 12 del GDPR. Questa lettura risulta indispensabile per quella che è l'analisi della sentenza *Schrems II*. Fondamentale, alla luce di questa nuova regolamentazione della disciplina, è il considerando n. 4. Questo ribadisce che:

> "[i]l trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità. Il presente regolamento rispetta tutti i diritti fondamentali e osserva le libertà e i principi riconosciuti dalla Carta, sanciti dai trattati, in particolare il rispetto della vita privata e familiare, del domicilio e delle comunicazioni, la protezione dei dati personali, la libertà di pensiero, di coscienza e di religione, la libertà di espressione e d'informazione, la libertà d'impresa, il diritto a un ricorso effettivo e a un giudice imparziale, nonché la diversità culturale, religiosa e linguistica"[69].

Il GDPR costituisce, in ultimo, l'approdo a una regolamentazione più dettagliata e aggiornata della materia. Grazie all'appello di Schrems, si pose il quesito circa il trattamento dei dati nei paesi terzi, evidenziando così un'attitudine differente verso il trattamento degli stessi. Nell'Unione europea la materia si consacra come tutelante dei diritti dei cittadini, mentre quella americana si frappone in una lettura dei cittadini – europei e non – come consumatori della rete dei dati[70]. Alla luce di siffatte discrepanze, il GDPR propone una nuova lettura del cittadino-consumatore, nell'ottica di un'integrazione economica e sociale sempre più globalizzata[71].

Questa concezione della nozione di consumatore non si distacca però dalla rigida tutela dei dati proposta dall'Unione europea. Invero, questo concetto si pone alla base di una circolazione dei dati – se adeguatamente tutelati – più libera e del completo sfruttamento delle tecnologie, in un'ottica che permane garantistica. Tale concetto risulta rimarcato adeguatamente ai considerando n. 6 e 7 del GDPR:

> "[l]a rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e

---

[67] Sentenza della Corte di giustizia del 13 maggio 2014, causa C-131/12, *sul diritto all'oblio, Google Spain e Google*.
[68] Regolamento (UE) 2016/679.
[69] *Ibidem*.
[70] R. F. JØRGENSEN, T. DESAI (2017: 106 ss).
[71] Regolamento (UE) 2016/679.

della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. […] La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali.
Tale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche"[72].

Nei paragrafi precedenti si ribadisce l'importanza del flusso transnazionale di dati nel contesto digitalizzato e globale dei rapporti economici. Nondimeno, alla base della dottrina europea permangono la tutela, la sicurezza e la trasparenza del trattamento dei dati. Infatti, il GDPR regola espressamente il trasferimento dei dati verso Paesi terzi o verso organizzazioni internazionali. Nell'ottica di un rafforzamento del quadro europeo e internazionale, si inserisce una novità fondamentale. All'art. 3, co. 1, si ricorda che:

> "[i]l presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione"[73].

La necessità di proporre un modello forte di tutela incrocia una flessibilità "[nell'] accogliere un 'approccio orientato verso i destinatari del servizio', estendendo dunque il suo ambito di applicazione, con una maggiore attenzione nei confronti della tutela dei soggetti interessati dal trattamento dei dati"[74].

Viene inoltre chiarito il concetto di adeguatezza, alla luce della giurisprudenza europea in materia. In proposito si ricorda che:

> "[i]l concetto di adeguatezza è, dunque, rivisto alla luce della pronuncia chiarendo in modo puntuali e più rigoroso gli elementi da valutare per porre in essere la decisione da parte della Commissione, tra di essi sono indicati: la tutela di diritti e libertà fondamentali, rimedi giurisdizionali previsti per la risoluzione di violazioni dei diritti stessi, la pertinente legislazione settoriale e generale, l'esistenza ed effettivo funzionamento di un'autorità indipendente a protezione dei dati personali nel Paese terzo con efficaci poteri sull'organizzazione internazionale destinataria dei dati; sono anche valutati gli impegni internazionali assunti dal Paese terzo dalle organizzazione che raccolgono i dati personali e strumenti giuridici vincolanti per la loro salvaguardia"[75].

---

[72] Regolamento (UE) 2016/679.
[73] *Ibidem*.
[74] M. G. STANZIONE (2016: 30).
[75] F. JAULT-SESEKE, C. ZOLYNSKI (2016: 1878); F. ACCARDO (2017: 171).

La tutela risulta ancora una volta la priorità nell'Unione. Soprattutto nell'ottica della letteratura giurisprudenziale, che vede il sovrapporsi "[of] the concept of personal data under the EU legislation […] to the notion of identity"[76]. I dati costituiscono cioè quello che si può definire il concetto di "individuo identificabile" e per tale ulteriore motivazione l'Unione europea si occupa di tutelarli in maniera stringente.

L'insieme delle considerazioni e delle novità apportate dal GDPR mettono ancora una volta in evidenza la differenza di protezione e il diverso uso che viene fatto dei dati. Nella prospettiva europea la tutela dei dati personali ha una rilevanza fondamentale, soprattutto in questa nuova ottica commerciale, sia all'interno dell'Unione che nel trasferimento verso paesi terzi. Mentre negli Stati Uniti d'America i dati vengono subordinati a una visione di "merce", volta unicamente al commercio e agli scambi. La tutela nell'Unione, anche alla luce degli art. 7 e 8 della Carta, rimane invece l'obiettivo centrale e non negoziabile.

[76] A. MONTI, R. WACKS (2019: 45).

Capitolo II

La sentenza 16 luglio 2020, causa C-311/18: *Commissario per la protezione dei dati c. Facebook Irlanda e Maximillian Schrems*

2.1 La sentenza *Schrems II*

La c.d. sentenza *Schrems II*[77] aveva ad oggetto la domanda di pronuncia pregiudiziale proposta, *ex* art. 267 TFUE, alla Corte di giustizia dell'Unione europea dalla Corte d'appello irlandese nella causa C-311/18. Tale domanda è stata avanzata in un'ottica di continuità con la controversia sorta nella sentenza *Schrems I*. Entrambe, infatti, hanno visto protagonisti il *Data Protection Commissioner* (*Commissioner*) contro Facebook Ireland Ltd e Maximilian Schrems. Come ricordato nella precedente sentenza, Schrems era un utente di Facebook che ha richiesto al *Commissioner* di esaminare i trasferimenti dei suoi dati personali dalla sede di Facebook Ireland alla sede principale, Facebook Inc, ubicata negli Stati Uniti.

La sentenza *Schrems II* si può quindi identificare come una seconda fase di denuncia, in rapporto alla precedente sentenza del 6 ottobre 2015[78]. Tale elemento di continuità si ritrova esplicitamente anche in sentenza, in quanto si rimanda in più punti all'analogia con la giurisprudenza della Corte in merito alla sentenza *Schrems I*. Quest'ultima aveva portato la Corte di giustizia a dichiarare invalida la decisione 2000/520/CE e a sostituire gli accordi che regolavano il flusso di dati tra l'Unione europea e gli Stati Uniti. Al *Safe Harbour Agreement* era subentrato il *Privacy Shield*. Entrambi erano volti a trasferire i dati personali dei cittadini europei al di fuori dei confini dell'Unione in un regime di tutela che fosse equivalente a quello riconosciuto dalla normativa europea.

A livello normativo, oltre agli accordi citati, tale trasferimento di dati verso i paesi terzi veniva formalmente garantito dalla decisione 2010/87/UE della Commissione europea circa l'avvio delle clausole contrattuali tipo (CCT) o *Standard Contractual Clauses* (SCC)[79]. Successivamente all'abrogazione della direttiva 95/46, all'art. 46 del GDPR tali clausole contrattuali prendono il nome di "clausole tipo di protezione". Infatti, in merito alla sentenza, Schrems aveva sostenuto che l'accordo tra le due società non fosse in linea con le clausole tipo di protezione e che tale regime non legittimasse un siffatto trasferimento dei dati verso gli Stati Uniti[80]. Secondo quanto menzionato dallo

---

[77] Sentenza della Corte di giustizia dell'Unione europea del 16 luglio 2020, causa C-311/18, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems*.
[78] S. FANTIN (2020: 5).
[79] Decisione della Commissione europea del 5 febbraio 2010, 2010/87, *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/CE del Parlamento europeo e del Consiglio*.
[80] S. FANTIN (2020: 5).

stesso Schrems circa la normativa statunitense, le imprese ubicate negli Stati Uniti avrebbero comunque dovuto consentire l'accesso da parte dei servizi di *intelligence* statunitensi ai database di Facebook.

In questo senso, successivamente alla sentenza *Schrems I*, il giudice del rinvio ha riconosciuto la denuncia di Schrems e l'ha rinviata al *Commissioner*. Lo stesso giudice ha sorretto la tesi portata avanti da Schrems circa l'ingerenza e la prassi di sorveglianza posta in essere dalle autorità statunitensi. Infatti, il giudice ha raccolto le prove delle operazioni dei programmi PRISM e UPSTREAM e ha rintracciato il fondamento giuridico delle attività di sorveglianza portate avanti delle autorità. Egli ha individuato la base legale di tali attività nell'art. 702 del *Foreign Intelligence and Surveillance Act* o FISA (S702) e nell'*Executive order 12333* (EO12333)[81]. In questo senso, il giudice del rinvio ha riconosciuto quello che è stato definito un sistema operante in senso "duraturo e indiscriminato"[82] dei dati personali, nonché la mancanza di garanzie e rimedi efficaci per i cittadini dell'Unione. Nello specifico, circa l'art. 702 del FISA, il giudice del rinvio ha precisato che questo consentisse alle autorità statunitensi di sorvegliare i cittadini stranieri che si trovassero anche al di fuori del territorio degli Stati Uniti. Nei fatti tale articolo era il fondamento giuridico dei programmi di sorveglianza PRISM e UPSTREAM[83]. Secondo lo stesso giudice, l'EO12333 permetteva altresì alle agenzie come la NSA di accedere a dati in transito verso gli Stati Uniti. Questo ordine consentiva di raccogliere e conservare tali dati prima che essi giungessero nel territorio statunitense e che fossero soggetti alle disposizioni del FISA una volta giunti nella giurisdizione statunitense. Inoltre, il giudice ha precisato che le attività fondate sull'EO12333 non fossero disciplinate dalla legge[84]. Di conseguenza, la legislazione statunitense prevedeva una disciplina differenziata per i dati trasferiti che consentisse le ingerenze da parte delle autorità sia durante il trasferimento che una volta approdati.

Nell'ambito dell'indagine aperta dal *Commissioner*, Facebook Ireland ha chiarito che i dati personali degli utenti fossero trasferiti a Facebook Inc. sulla base della decisione 2010/87 sulle clausole contrattuali tipo. Alla luce di tali indagini, Schrems ha chiesto al *Commissioner* di sospendere i trasferimenti verso gli Stati Uniti. Tuttavia, lo stesso *Commissioner* ha stabilito che non si potesse dare una decisione circa il livello di protezione garantito dagli Stati Uniti d'America in merito alle clausole contrattuali tipo, senza che prima la Corte si pronunciasse sulla validità della decisione 2010/87.

---

[81] Sentenza della Corte di giustizia *Schrems II*, punto 60.

[82] M. NINO (2013: 727 ss.).

[83] Sentenza della Corte di giustizia *Schrems II*, punto 62: "[p]er quanto riguarda il programma UPSTREAM, detto 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 da un «selettore». Nell'ambito di tale programma, la NSA, secondo le constatazioni del medesimo giudice, ha accesso tanto ai metadati quanto al contenuto delle comunicazioni interessate".

[84] Ivi, punto 63.

Tenuto conto di tali elementi il *Commissioner* ha invitato Schrems a riformulare la sua denuncia. Il 10 dicembre 2015 Schrems ha presentato la denuncia riformulata, supportando la tesi che il diritto statunitense consentisse a Facebook Inc. di mettere a disposizione delle autorità americane, quali la *National Security Agency* (NSA), il *Federal Bureau of Investigation* (FBI) e la *Central Intelligence Agency* (CIA)[85], tutti i dati che fossero trasferiti nel territorio statunitense. Egli ha sostenuto che, poiché tali dati venivano utilizzati nell'ambito di diversi programmi di sorveglianza in modo incompatibile con gli articoli 7, 8, e 47 della Carta, la decisione 2010/87 non potesse legittimare il flusso dei suddetti dati verso gli Stati Uniti. Schrems ha pertanto chiesto al *Commissioner* di vietare, o almeno di sospendere, il trasferimento dei suoi dati personali verso la società statunitense. In risposta, il 24 maggio 2016 il *Commissioner* ha emanato delle conclusioni provvisorie, nelle quali ha considerato che i dati dei cittadini dell'Unione trasferiti negli Stati Uniti corressero il rischio di essere esaminati e trattati dalle autorità statunitensi, incompatibilmente con gli articoli 7 e 8 della Carta. Egli ha inoltre stabilito che il diritto interno statunitense non concedesse ai cittadini dei mezzi di ricorso conciliabili con l'art. 47 della Carta[86].

In tali circostanze, ritenendo che la denuncia riformulata da Schrems sollevasse la questione della validità della decisione 2010/87, il 31 maggio 2016 il *Commissioner* ha adito la Corte d'appello irlandese, affinché questa si rivolgesse alla Corte di giustizia circa tale controversia. Di conseguenza, con un provvedimento del 4 maggio 2018, la Corte d'appello irlandese ha sospeso il procedimento principale, sottoponendo undici questioni pregiudiziali alla Corte di giustizia dell'Unione europea[87]. Tali questioni sono state sollevate: in merito alla competenza delle autorità preposte alla protezione dei dati nel caso in cui si riscontrino delle carenze sistemiche; circa l'applicabilità del diritto dell'Unione nelle attività di sicurezza nazionale al di fuori della giurisdizione europea; circa l'interpretazione e la validità della decisione 2010/87 sulle clausole contrattuali tipo; sulla validità della decisione di esecuzione 2016/1250 sull'adeguatezza della protezione offerta del *Privacy Shield*[88].

Tuttavia, occorre specificare il contesto normativo alla luce del quale la Corte di giustizia si è pronunciata in sentenza. Infatti, più volte all'interno delle questioni pregiudiziali si fa riferimento alla direttiva 95/46/CE. Invece, sull'applicabilità *ratione temporis* della direttiva sopracitata in sentenza è stato specificato che, avendo il GDPR *ex* art. 99 sovrascritto tale direttiva, per rispondere alle questioni pregiudiziali si doveva far riferimento alle disposizioni del GDPR, e non a quelle della direttiva[89]. Quindi, il contesto normativo in cui la sentenza si è sviluppata tiene conto del GDPR. Questo regge quelli che sono i punti cardine della protezione dei dati, nell'ottica di un'evoluzione tecnologica rapida, della globalizzazione e di un elevato e coerente livello di

[85] Sentenza della Corte di giustizia *Schrems II*, punto 61.
[86] Ivi, punto 56.
[87] Ivi, punto 57.
[88] S. FANTIN (2020: 2).
[89] Sentenza della Corte di giustizia *Schrems II*, punto 79.

protezione che dovrebbe essere equivalente in tutti gli Stati membri[90]. Peraltro, alla luce della sentenza *Schrems I*, la parte centrale del regolamento, a partire dal suo art. 44 fino all'art. 50, verte sulle considerazioni circa il trasferimento transfrontaliero. In sentenza, si menziona nuovamente la possibilità di trasferire i dati verso Paesi terzi, con una disciplina nuova e rafforzata. Ai considerando numeri 103, 107, 108 viene sottolineato come il livello di adeguatezza sia ancora il perno fondamentale della disciplina[91]. Come ricordato poi al considerando n. 104, il paese terzo verso cui i dati vengono trasferiti dovrebbe quantomeno essere in linea con i valori fondamentali su cui l'Unione europea è istituita e dovrebbe offrire delle garanzie di un livello di protezione sostanzialmente equivalente a quello promosso dall'Unione. Inoltre, il trattamento dei dati deve essere sottoposto a un controllo intransigente delle autorità, consentendo all'interessato di esercitare

> "[i]l diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento il diritto a un ricorso giurisdizionale effettivo a norma dell'articolo 47 della Carta qualora ritenga che siano stati violati i diritti di cui gode a norma del presente regolamento"[92].

Circa la prima questione pregiudiziale il giudice del rinvio domandava se il diritto dell'Unione fosse applicabile ai dati personali trasferiti a fini commerciali verso un altro Stato che potesse trattarli a fini di sicurezza nazionale. Ci si chiedeva infatti

> "1) [s]e, in circostanze in cui dati personali sono trasferiti da una società privata di uno Stato membro dell'[Unione] a una società privata in un paese terzo per scopi commerciali ai sensi della [decisione 2010/87] e possono essere ulteriormente trattati nel paese terzo dalle sue autorità ai fini della sicurezza nazionale ma anche ai fini dell'applicazione della legge e della gestione della politica estera del paese terzo, il diritto dell'Unione, compresa la Carta, sia applicabile al trasferimento dei dati, nonostante le disposizioni di cui all'articolo 4, paragrafo 2, TUE in relazione alla sicurezza nazionale e le disposizioni di cui al primo trattino dell'articolo 3, paragrafo 2, della [direttiva 95/46] in relazione alla pubblica sicurezza, alla difesa e alla sicurezza dello Stato"[93].

In sentenza, la Corte si è espressa circa la possibilità di applicazione del GDPR a dati, trasferiti o in trasferimento, che subissero un trattamento da parte delle autorità del paese terzo interessato a fini di pubblica sicurezza. Infatti, secondo la Corte, tali dati non esulano dalla competenza del regolamento

---

[90] Regolamento (UE) del Parlamento europeo e del Consiglio, del 27 aprile 2016, 2016/679, *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*, considerando n. 6 e n. 10.
[91] Sentenza della Corte di giustizia *Schrems II*, punto 8.
[92] Regolamento (UE) 2016/679, considerando n. 141.
[93] Sentenza della Corte di giustizia *Schrems II*, punto 68.

europeo[94]. Pertanto, ai sensi dell'art. 2, paragrafi 1 e 2, del GDPR[95], si doveva affermare che il flusso di dati da uno Stato membro verso uno Stato terzo volto a fini commerciali rientrasse nella sfera di applicazione dello stesso regolamento, nonostante l'ipotesi che tali dati subissero poi un trattamento da parte delle autorità per questioni di sicurezza pubblica, difesa e sicurezza dello Stato.

Circa le questioni seconda, terza e sesta il giudice del rinvio interrogava la Corte circa il livello di protezione richiesto dalle clausole tipo di protezione nell'ambito di un trasferimento di dati, come stabilito all'art. 46, paragrafi 1 e 2, del GDPR. In sostanza, cioè, il giudice chiedeva alla Corte di stabilire quali fossero gli elementi per determinare se tali clausole garantissero un livello di protezione adeguato in materia di trasferimento. Nello specifico, la sesta questione pregiudiziale trattava proprio il livello di protezione richiesto dalle clausole tipo di protezione in un contesto di *transborder data flow*[96] tra uno Stato membro e uno Stato terzo.

Di conseguenza, veniva sancito che, per determinare se il trasferimento garantisse un livello di protezione adeguato, non bastasse valutare solamente le clausole convenute tra i sottoscrittori. Infatti, è stato sottolineato che andasse preso in considerazione anche l'apparato giudiziario del paese terzo considerato. L'art. 45, par. 2, del GDPR[97] evidenzia quali sono i requisiti che

---

[94] Sentenza della Corte di giustizia *Schrems II*, punto 86.

[95] L'art. 2, paragrafi 1 e 2, del regolamento 2016/679 stabilisce che: "1. [i]l presente regolamento si applica al trattamento interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi. 2. Il presente regolamento non si applica ai trattamenti di dati personali: a) effettuati per attività che non rientrano nell'ambito di applicazione del diritto dell'Unione; b) effettuati dagli Stati membri nell'esercizio di attività che rientrano nell'ambito di applicazione del titolo V, capo 2, TUE; c) effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico; d) effettuati dalle autorità competenti a fini di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro minacce alla sicurezza pubblica e la prevenzione delle stesse".

[96] C. KUNER (2012: 215).

[97] L'art. 45, par. 2, del regolamento 2016/679 stabilisce che: "[…] a) lo stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale osservate nel paese o dall'organizzazione internazionale in questione, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento; b) l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri; e c) gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali".

lo Stato destinatario deve possedere al fine consentire una completa valutazione della Commissione sul grado di protezione dello Stato terzo. Infatti, come ribadito in sentenza, uno degli obiettivi posti agli articoli 45 e 46 del GDPR sui trasferimenti dei dati all'estero è di assicurare una continuità delle salvaguardie. In entrambe le sentenze *Schrems* questa continuità delle salvaguardie viene definita come "sostanziale equivalenza". Secondo quanto ricordato dalla Corte e dagli avvocati generali di entrambe le sentenze, bisogna assicurare una continuità di protezione che si esplica oltre i confini dell'Unione europea. Per contro, la sostanziale equivalenza può essere assicurata anche attraverso dei mezzi differenti da quelli utilizzati dall'Unione, ma si deve riuscire a rintracciare nel risultato finale. Si dovrebbe trattare, nella sostanza, di un livello di tutela comparabile. In merito al punto sesto, l'avvocato generale Saugmandsgaard Øe ha ribadito che "il modo in cui viene preservata la continuità dell'elevato livello di protezione varia a seconda della base giuridica del trasferimento"[98].

Perciò, laddove l'art. 46, par. 1, del GDPR autorizzasse il trasferimento di dati personali anche verso Stati terzi che non salvaguardassero adeguatamente i dati personali importati, la disposizione consentiva simili trasferimenti esclusivamente quando garantiti con altri strumenti. Le clausole tipo di protezione costituivano in questo senso "un meccanismo generale applicabile ai trasferimenti indipendentemente dal paese terzo di destinazione e dal livello di protezione ivi garantito"[99].

Per rispondere alle questioni seconda, terza e sesta la Corte di giustizia ha stabilito che l'art. 46, paragrafi 1 e 2, lett. c), doveva essere letto

> "[…] l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento"[100].

Relativamente alle questioni quarta e quinta, il giudice del rinvio chiedeva se il flusso di dati personali verso gli Stati Uniti, fondato sulla decisione 2010/87, violasse i diritti garantiti dagli articoli 7, 8 e 47 della Carta. Inoltre, l'esame della Corte doveva prendere in considerazione anche le conseguenze

---

[98] Conclusioni dell'Avvocato generale Saugmandsgaard Øe *Schrems II*, punto 118.
[99] Ivi, punto 120.
[100] Sentenza della Corte di giustizia *Schrems II*, punto 105.

derivanti dall'adozione del *Privacy Shield*, sopraggiunto nel frattempo. In proposito, la nona questione domandava quale fosse la posizione delle autorità di controllo degli Stati membri e se il paese terzo garantisse un livello di protezione adeguato, stando a quanto stabilito nell'accordo. Nonché lo stesso giudice domandava, alla decima questione, se ci fosse compatibilità tra l'Ombudsperson[101], menzionato nel *Privacy Shield*, e l'art. 47 della Carta. Sostanzialmente il giudice del rinvio interrogava l'adeguatezza del *Privacy Shield*, sottoponendo le citate questioni pregiudiziali. Queste mettevano in discussione il fatto che gli Stati Uniti garantissero un livello di protezione adeguato dei dati personali trasferiti dall'Unione verso tale paese e, pertanto, la validità della decisione[102].

Dunque, al fine di risolvere la controversia di cui al procedimento principale, si doveva tener conto del mutamento delle circostanze nel quadro giuridico europeo, relativamente all'adozione del *Privacy Shield*. Come disposto dall'art. 1, par. 1, dell'accordo e come ricordato alle questioni seconda, terza e sesta, bisognava accertare che gli Stati Uniti garantissero un livello di protezione adeguato affinché i dati vi fossero legittimamente trasferiti. Effettivamente, questo era richiesto ai fini della valutazione degli obblighi che incombevano sull'autorità di controllo[103]. Infatti, nel caso in cui si fosse constatato che gli Stati Uniti avessero garantito un livello di protezione adeguato, il margine di intervento da parte delle autorità veniva automaticamente limitato dal *Privacy Shield*. Di conseguenza, un livello considerato adeguato avrebbe autorizzato il flusso di dati senza ulteriori garanzie d'azione. Sostanzialmente, l'autonomia di accertamento delle autorità consentiva loro di sospendere o vietare il trasferimento nel caso in cui si fosse appurato che il livello di protezione dei dati non fosse stato idoneo. Pertanto, fino a che la Corte non avesse dichiarato invalida la decisione che istituiva il *Privacy Shield*, l'autorità di controllo competente non avrebbe potuto sospendere o vietare il trasferimento di dati verso un'organizzazione o un paese che avesse aderito all'accordo[104].

Ai sensi dell'art. 77, par. 1, del GDPR, se un individuo crede che lo Stato verso cui i suoi dati vengono trasferiti non dia le adeguate garanzie, può fare un esposto all'autorità di controllo competente. Allora, quest'ultima indaga in piena indipendenza se il trasferimento di dati personali osservi il regolamento. Laddove l'autorità ritenga fondato il reclamo deve "proporre un ricorso dinanzi ai giudici nazionali affinché questi ultimi sottopongano alla

[101] Letteralmente "mediatore", un tipo di figura che opera a stretto contatto con enti amministrativi e le cui competenze vengono riportate nella decisione di esecuzione (UE) 2016/1250, dal considerando n. 116 al n. 122.
[102] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe del 19 dicembre 2019, causa C-311/2018, *Data Protection Commissioner contro Facebook Ireland Limited, Maximillian Schrem*, punto 175.
[103] Sentenza della Corte di giustizia *Schrems II*, punto 154.
[104] Ivi, punto 156.

Corte un rinvio pregiudiziale ai fini della valutazione della validità della suddetta decisione"[105].

In sostanza, per poter fornire una risposta completa sulla questione, la Corte doveva esaminare se il *Privacy Shield* facesse fede alla regolamentazione europea fondata sul GDPR. In sentenza, al punto 160 viene detto che,

> "[c]ome rilevato dall'avvocato generale al paragrafo 175 delle sue conclusioni, tali questioni pregiudiziali devono quindi essere intese nel senso che esse mettono in discussione, in sostanza, la constatazione della Commissione, contenuta nella decisione «scudo per la privacy», secondo la quale gli Stati Uniti garantiscono un livello adeguato di protezione dei dati personali trasferiti dall'Unione verso tale paese terzo e, pertanto, la validità di tale decisione"[106].

L'analisi dell'accordo e dell'adeguatezza di protezione garantita dagli Stati Uniti ha consentito di rilevare che tale ordinamento giuridico risultasse manchevole di qualsiasi mezzo di ricorso per i cittadini. Infatti, qualora essi volessero avvalersi di basi giuridiche volte a contrastare le ingerenze da parte delle autorità di *intelligence*, le garanzie statunitensi non avrebbero consentito di mettere in atto tale ricorso. Ovvero risultava che

> "[…] né l'articolo 702 del FISA, né l'E.O. 12333, in combinato disposto con la PPD-28, corrispondono ai requisiti minimi connessi, nel diritto dell'Unione, al principio di proporzionalità, cosicché non si può considerare che i programmi di sorveglianza basati su tali disposizioni siano limitati allo stretto necessario[107]".

Per cui, una simile lacuna nella tutela impedisce di stabilire "che il diritto degli Stati Uniti garantisce un livello di protezione sostanzialmente equivalente a quello garantito dall'articolo 47 della Carta"[108]. Per tali ragioni "si deve concludere che la decisione «scudo per la privacy» è invalida"[109].

All'ottava questione, il giudice del rinvio chiedeva come dovesse essere interpretato l'art. 58, par. 2, lettere f) e j), del GDPR. Il giudice domandava se tale articolo chiedesse che l'autorità di controllo fosse tenuta a sospendere o a vietare un trasferimento di dati effettuato sulla base di clausole contrattuali, nel caso in cui avesse ritenuto che queste non fossero rispettate nel paese terzo. Ovvero se lo stesso paese non garantisse la protezione dei dati trasferiti richiesta dal diritto dell'Unione, in particolare dagli articoli 45 e 46 del GDPR e dalla Carta. Oppure se chiedesse che l'esercizio di tali poteri da parte delle autorità di controllo fosse limitato ad ipotesi eccezionali[110]. Infatti, come è stato detto in specifica ai punti precedenti della sentenza, il ruolo delle attività di controllo è di verificare se un determinato trasferimento avviene secondo i requisiti e i criteri di applicazione del GDPR. Ai sensi dell'art. 57, par. 1, lett. f), dell'art. 77, par. 1, e dell'art. 78, paragrafi 1 e 2, del GDPR l'autorità di

---

[105] Sentenza della Corte di giustizia *Schrems II*, punto 157.
[106] Ivi, punto 160.
[107] Ivi, punto 184.
[108] Ivi, punto 191.
[109] Ivi, punto 201.
[110] Ivi, punto 106.

controllo deve procedere al trattamento di un reclamo da parte dei cittadini dell'Unione europea in maniera indipendente e con tutta la diligenza richiesta[111].

Per rispondere all'ottava questione l'avvocato generale Saugmandsgaard Øe a tal riguardo ha rilevato che:

> "[…] in forza dell'articolo 58, paragrafo 2, lettere f) e j), di tale regolamento, tale 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 tipo 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 il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo"[112].

Inoltre, ai sensi dell'art. 288, par. 4, TFUE, è stata sottolineata l'obbligatorietà della decisione in tutti i suoi elementi e per tutti i destinatari designati. Di conseguenza, constatando un livello di protezione adeguato nello Stato terzo, si forniva la legittimazione dei trasferimenti dei dati[113]. Per cui

> "[…] finché la decisione di adeguatezza non fosse stata dichiarata invalida dalla Corte, gli Stati membri e i loro organi, fra i quali figurano le loro autorità di controllo indipendenti, non possono adottare misure contrarie a tale decisione, quali atti intesi a constatare con effetto vincolante che il paese terzo interessato da detta decisione non garantisce un livello di protezione adeguato"[114].

Pertanto, per rispondere a tale questione la Corte ha dichiarato che l'interpretazione dell'art. 58, par, 2, lettere f) e j), del GDPR identificava la competenza dell'autorità di controllo a sospendere o vietare i trasferimenti dei dati dei cittadini europei verso Stati terzi, eseguiti sulla base di clausole tipo di protezione. Nel caso in cui un'autorità di controllo avesse ritenuto che le clausole non fossero state rispettate nello Stato di approdo e che la protezione dei dati richiesta dagli articoli 45 e 46 del GDPR non potesse essere garantita nello stato oggetto del trasferimento allo stesso modo del diritto dell'Unione, allora le autorità avrebbero dovuto sospendere o mettere fine al trasferimento.

Le questioni settima e undicesima riguardavano la "validità della decisione 2010/87 alla luce degli articoli 7, 8 e 47 della Carta"[115]. Di conseguenza, l'avvocato generale fornisce una risposta alla settima e undicesima questione stabilendo che la validità della decisione 2010/87 non dipende dal livello di protezione del paese terzo, bensì dalla solidità delle clausole tipo di protezione. Queste dovrebbero infatti compensare eventuali carenze[116]. Il fatto che le clausole non fossero vincolanti per le autorità dei paesi terzi non invalidava

---

[111] Sentenza della Corte di giustizia *Schrems II*, punti da 107 a 110.
[112] Ivi, punto 113.
[113] Ivi, punto 117.
[114] Ivi, punto 118.
[115] Conclusioni dell'Avvocato generale Saugmandsgaard Øe *Schrems II*, punto 121.
[116] Ivi, punto 124.

di per sé la decisione 2010/87[117]. In sentenza è stato stabilito che è dovere dell'esportatore effettuare un monitoraggio continuo della normativa del paese terzo in funzione di un ipotetico mutamento delle circostanze in tale paese terzo. Nel caso in cui i soggetti interessati subissero una violazione dei dati, delle garanzie di tutela vengono previste formalmente dalle clausole e dall'art. 58, par. 2, del GDPR. Dal punto di vista del controllo, queste ulteriori questioni hanno sancito che il potere di sospendere il trasferimento si dovesse dichiarare come un obbligo delle autorità di protezione dei dati nel caso in cui non si fossero manifestate le condizioni adeguate al trasferimento[118]. Mentre qualsiasi decisione che limitasse i diritti degli interessati sarebbe stata soggetta a controllo giudiziario[119].

Conseguentemente all'esame della decisione 2010/87, la Corte di giustizia ha risposto alle due questioni dichiarando che, alla luce degli articoli 7, 8 e 47 della Carta, la decisione non fosse invalidata da alcun elemento.

Per questi motivi, la Corte, riunitasi in Grande Sezione, ha dichiarato che

> "1) [l]'articolo 2, paragrafi 1 e 2, del 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, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati), deve essere interpretato nel senso che rientra nell'ambito di applicazione di tale regolamento un trasferimento di dati personali effettuato a fini commerciali da un operatore economico stabilito in uno Stato membro verso un altro operatore economico stabilito in un paese terzo, nonostante il fatto che, durante o in seguito a tale trasferimento, i suddetti dati possano essere sottoposti a trattamento da parte delle autorità del paese terzo considerato a fini di sicurezza pubblica, di difesa e sicurezza dello Stato.
>
> 2) L'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del regolamento 2016/679 devono essere interpretati nel senso che le garanzie adeguate, i diritti azionabili e i mezzi di ricorso effettivi richiesti da tali disposizioni devono garantire che i diritti delle persone i cui dati personali sono trasferiti verso un paese terzo sul fondamento di clausole tipo di protezione dei dati godano di un livello di protezione sostanzialmente equivalente a quello garantito all'interno dell'Unione da tale regolamento, letto alla luce della Carta dei diritti fondamentali dell'Unione europea. A tal fine, la valutazione del livello di protezione garantito nel contesto di un trasferimento siffatto deve, in particolare, prendere in considerazione tanto le clausole contrattuali convenute tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo interessato quanto, per quel che riguarda un eventuale accesso delle autorità pubbliche di tale paese terzo ai dati personali così trasferiti, gli elementi rilevanti del sistema giuridico di quest'ultimo, in particolare quelli enunciati all'articolo 45, paragrafo 2, di detto regolamento.
>
> 3) L'articolo 58, paragrafo 2, lettere f) e j), del regolamento 2016/679 deve essere interpretato nel senso che, a meno che esista una decisione di

[117] S. FANTIN (2020: 3).
[118] Conclusioni dell'Avvocato generale Saugmandsgaard Øe *Schrems II*, punti 143 e 146.
[119] Ivi, punto 155.

> adeguatezza validamente adottata dalla Commissione europea, l'autorità di controllo competente è tenuta a sospendere o a vietare un trasferimento di dati verso un paese terzo effettuato sulla base di clausole tipo di protezione dei dati adottate dalla Commissione, qualora detta autorità di controllo ritenga, alla luce del complesso delle circostanze proprie di tale trasferimento, che le suddette clausole non siano o non possano essere rispettate in tale paese terzo e che la protezione dei dati trasferiti richiesta dal diritto dell'Unione, segnatamente dagli articoli 45 e 46 di tale regolamento e dalla Carta dei diritti fondamentali, non possa essere garantita con altri mezzi, ove il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione non abbiano essi stessi sospeso il trasferimento o messo fine a quest'ultimo.
>
> 4) Dall'esame della 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/CE del Parlamento europeo e del Consiglio, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali non è emerso alcun elemento idoneo ad inficiarne la validità.
>
> 5) La decisione di esecuzione (UE) 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy, è invalida"[120].

2.2 La Corte di giustizia dell'Unione Europea e l'invalidità della decisione 2016/1250

La Corte di giustizia dell'Unione europea con la sentenza del 16 luglio 2020 nella causa C-311/18 ha dichiarato invalida la decisione di esecuzione 2016/1250 della Commissione. Tale decisione stabiliva l'adeguatezza del *Privacy Shield* come accordo regolatore del *transborder data flow* dall'Unione europea verso gli Stati Uniti. In particolare, l'accordo si poneva a garanzia di un livello idoneo di tutela dei dati personali. Il *Privacy Shield* si basava su un sistema di adesione volontario da parte delle aziende locate negli Stati Uniti, tramite un meccanismo di autocertificazione per cui

> "[…] l'organizzazione statunitense s'impegna a rispettare un insieme di principi in materia di privacy, ossia i principi del regime dello Scudo UE-USA per la privacy, comprensivi dei principi supplementari, emanati dal Dipartimento del Commercio degli USA"[121].

I pilastri fondamentali dell'accordo erano quattro: gli obblighi imposti a chi aderiva all'accordo; garanzie che questi fossero rispettati; una stringente e prevista tutela da parte delle autorità di controllo; nonché il monitoraggio congiunto della Commissione insieme con il *Department of Commerce*[122].

---

[120] Sentenza della Corte di giustizia, *Schrems II*.
[121] Decisione di esecuzione (UE) 2016/1250, considerando n. 14.
[122] P. PIRODDI, (2016: 196 ss.); S. SICA, V. D'ANTONIO (2016: 165 ss.); F. ACCARDO (2017: 167).

In osservanza del *Privacy Shield*, gli impegni presi dal governo statunitense hanno dato vita ad un nuovo ente, il c.d Ombudsperson[123] o mediatore. Questo era un organo tramite il quale si poteva portare avanti un ricorso amministrativo, volto ad accertare che i servizi di *intelligence* osservassero quanto disposto dall'accordo. Come ricordato alla questione decima del rinvio pregiudiziale, questo era un soggetto indipendente che riceveva e indagava gli esposti dei cittadini, esercitando cioè un potere di vigilanza. Tale potere avrebbe dovuto porre rimedio alle situazioni di irregolarità in cui fossero incorse le pubbliche autorità. Motivo per cui, alla citata questione decima, ci si chiedeva se tale ente rispettasse l'art. 47 della Carta.

Il *Privacy Shield* appariva per un verso come un sistema nuovo predisposto dall'*U.S. Department of Commerce*, implementato delle garanzie che assicurassero la tutela dei dati trasferiti e in trasferimento. In un altro verso ha invece sollevato dei dubbi sul suo funzionamento e sulle autorità predisposte a occuparsi delle controversie in merito alla tutela. Il riferimento era infatti volto ad interrogarsi circa il ruolo dell'Ombudsperson, che nonostante fosse identificato come un ente indipendente e terzo, rimaneva comunque un'estensione dell'*U.S. Department of Commerce*[124].

Ecco che si è pervenuti a sollevare le questioni pregiudiziali di cui si è trattato. Pertanto, da ciò derivano le legittime preoccupazioni sull'effettività dell'accordo e sull'impatto circa la protezione dei dati personali dei soggetti. Circa l'art. 47 della Carta, sono stati analizzati sia l'efficacia dei mezzi giuridici degli Stati Uniti, che il meccanismo dell'Ombudsperson. In primo luogo, il *Privacy Shield* non prevedeva alcun vincolo da parte degli Stati Uniti di informare l'Unione europea nel caso in cui avessero dovuto avviare un sistema di sorveglianza nei confronti di qualche cittadino[125]. Nonché, i meccanismi extragiudiziali degli Stati Uniti menzionati dal sistema non disponevano di un'adeguata indipendenza tale da poter intraprendere revisioni imparziali. In secondo luogo, l'avvocato generale dubitava che l'Ombudsperson riuscisse a compensare le carenze della tutela legale statunitense in materia. Innanzitutto, perché l'ente veniva direttamente nominato dal Segretario di Stato, e inoltre per la non vincolatività delle decisioni emanate dallo stesso. Di conseguenza, tale istituto poteva solamente confermare l'esistenza di attività di sorveglianza, ma nulla poteva fare legalmente per correggere qualsiasi violazione le parti che stessero commettendo[126]. In sentenza viene infatti ribadito che

> "[s]econdo costante giurisprudenza, l'esistenza stessa di un controllo giurisdizionale effettivo, destinato a garantire il rispetto delle disposizioni del diritto dell'Unione, è intrinseca all'esistenza di uno Stato di diritto. Pertanto, una normativa che non prevede alcuna possibilità per il singolo di avvalersi di rimedi

[123] F. ROSSI DAL POZZO (2016: 721) sostiene che l'Ombudsperson sia una "figura sui generis, alto funzionario chiamato ad assicurarsi che le denunce dei singoli siano informati se le leggi degli Stati Uniti applicabili siano state rispettate o, qualora così non fosse, se le violazioni riscontrate siano cessate".
[124] S. CRESPI (2016: 261); F. ROSSI DAL POZZO (2016: 721); F. ACCARDO (2017: 169).
[125] S. FANTIN (2020: 3).
[126] *Ibidem*.

> giuridici al fine di accedere a dati personali che lo riguardano, oppure di ottenere la rettifica o la soppressione di tali dati, non rispetta il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva, quale sancito all'articolo 47 della Carta"[127].

Infatti, tale accordo è stato fortemente criticato in quanto non vincolava a sufficienza le aziende e le autorità statunitensi ad adempiere agli accordi stretti con l'Unione europea. Lo stesso Maximilian Schrems lo ha definito un "soft update of Safe Harbour [Agreement]"[128].

Pertanto, l'avvocato generale ha consigliato alla Corte di Lussemburgo di non rispondere a ulteriori questioni ritenute non necessarie per il caso. Successivamente ha formulato i motivi che lo portavano a mettere in discussione la validità della decisione 2016/1250, che istituiva il *Privacy Shield*. Ha suggerito che la valutazione circa l'adeguatezza dei paesi terzi effettuata dalla Commissione europea prima di una decisione di adeguatezza avrebbe dovuto valutare anche le potenziali interferenze delle attività di *intelligence* come se fossero state intraprese da uno Stato membro dell'UE.

In sentenza è infatti stato stabilito che

> "[i]n tali circostanze, le limitazioni alla protezione dei dati personali, che derivano dalla normativa interna degli Stati Unit in materia di accesso e utilizzo, da parte delle autorità pubbliche statunitensi, di tali dati trasferiti dall'Unione verso gli Stati Uniti e che la Commissione ha valutato nella decisione «scudo per la privacy», non sono inquadrate in modo da corrispondere a requisiti sostanzialmente equivalenti a quelli richiesti, nel diritto dell'Unione, dall'articolo 52, paragrafo 1, seconda frase, della Carta"[129].

È stata inoltre ribadita l'inadeguatezza del diritto interno statunitense, circa il FISA e l'EO12333, i quali non soddisfano i requisiti minimi del principio di proporzionalità. Infatti, sebbene i due strumenti perseguissero obiettivi di sicurezza, permanevano degli interrogativi sulla sufficiente specificità con cui fossero definite le limitazioni di intervento da parte delle autorità di sorveglianza nella regolamentazione statunitense. In ultima analisi, i due programmi non rispettavano le condizioni di necessità e proporzionalità richieste dall'Unione europea, a causa della mancanza di garanzie specifiche, di meccanismi di revisione adeguati e di regole procedurali stabilite in modo indipendente[130].

Anche l'istituzione dell'Ombudsperson non garantiva la terzietà, l'autonomia e l'indipendenza necessarie ad una tutela adeguata. Questo risultava infatti essere, come ricordato, un'estensione dell'*U.S. Department of Commerce* nonché per la non vincolatività delle decisioni emanate dallo stesso. Invece, un organo adeguatamente funzionante posto in uno Stato terzo era di cruciale importanza. Infatti, in sentenza si sottolinea che

---

[127] Sentenza della Corte di giustizia *Schrems II*, punto 187.
[128] M. SCHREMS (2016: 148 ss.).
[129] Sentenza della Corte di giustizia *Schrems II*, punto 185.
[130] S. FANTIN (2020: 3).

> "[l]'esistenza di tali effettive possibilità di ricorso nel paese terzo considerato riveste un'importanza particolare nel contesto di un trasferimento di dati personali verso tale paese terzo, in quanto, come risulta dal considerando 116 del RGPD, gli interessati possono trovarsi di fronte all'insufficienza dei poteri e dei mezzi delle autorità amministrative e giudiziarie degli Stati membri per poter dare utilmente seguito ai loro reclami fondati su un asserito trattamento illecito, in tale paese terzo, dei loro dati in tal modo trasferiti, il che può costringerli a rivolgersi alle autorità e ai giudici nazionali di siffatto paese terzo"[131].

Per tali motivazioni, la Corte, nella *Schrems II*, dichiara invalida la decisione di esecuzione 2016/1250 della Commissione, del 12 luglio 2016, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy[132].

2.3 La continuità delle *Standard Contractual Clauses*

Le clausole contrattuali tipo sono clausole stabilite dalle decisioni della Commissione e vengono incluse negli accordi che disciplinano l'esportazione di dati personali. Ovvero, sono dei contratti a cui aderisce l'importatore stabilito in uno Stato terzo, al di fuori dell'Unione europea[133]. Ad oggi vengono disciplinate in maniera esaustiva dall'art. 46, par. 2, lettere c) e d), del GDPR, come ribadito dalla Corte nella sentenza *Schrems II*. Infatti

> "4) [d]all'esame della 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/CE del Parlamento europeo e del Consiglio, come modificata dalla decisione di esecuzione (UE) 2016/2297 della Commissione, del 16 dicembre 2016, alla luce degli articoli 7, 8 e 47 della Carta dei diritti fondamentali non è emerso alcun elemento idoneo ad inficiarne la validità"[134].

Anteriormente alla sentenza *Schrems I*, la base giuridica dei trasferimenti transfrontalieri di dati si basava sull'adozione di tali clausole congiuntamente ai principi stabiliti dal *Safe Harbour Agreement*. Tuttavia, nonostante tale accordo fosse stato estinto dalla prima sentenza *Schrems*, le clausole contrattuali tipo sono rimaste validamente in vigore. Tuttavia, queste a seguito dell'abrogazione della direttiva 95/46, in cui erano menzionate all'art. 26, hanno assunto il nome di "clausole tipo di protezione"[135]. Tuttavia, la

---

131 Sentenza della Corte di giustizia *Schrems II*, punto 189.
132 Sentenza della Corte di giustizia *Schrems II*.
133 G. M. RICCIO (2016: 227).
134 Sentenza della Corte di giustizia *Schrems II*.
135 Lo stesso avvocato generale Saugmandsgaard Øe al punto 113 delle sue conclusioni stabilisce che: "[i]n tale contesto, la prima parte della sesta questione pregiudiziale invita la Corte a stabilire se l'applicazione delle «clausole contrattuali tipo» adottate dalla Commissione ai sensi dell'articolo 26, paragrafo 4, della direttiva 95/46 – corrispondenti alle «clausole tipo di protezione» ora menzionate all'articolo 46, paragrafo 2, lettera c), del RGPD – debba consentire di

disciplina delle stesse è rimasta vigente. Infatti, nonostante le molteplici analisi della decisione 2010/87 e delle garanzie poste in essere da questa, le clausole tipo di protezione non sono state invalidate dalla Corte di giustizia. Di conseguenza, si può desumere che le clausole sono state un efficace punto di contatto nella disciplina del flusso transfrontaliero di dati. Queste, insieme alle c.d. *binding corporate rules*, alle clausole contrattuali *ad hoc* così come disciplinate dall'art. 46, par. 3, lett. a), del GDPR, agli accordi tra *data importer* e *data exporter* e agli atti fondati sul consenso dell'interessato sono stati riscoperte come strumenti legali più idonei dei semplici accordi tra l'Unione europea e gli Stati Uniti[136]. Inoltre, tali strumenti sono stati implementati alla luce del nuovo regolamento europeo intercorso tra una sentenza e l'altra.

Essendo il focus degli accordi stipulati in seno all'Unione europea e gli Stati Uniti incentrato sul consenso dell'interessato, le imprese hanno dovuto trovare delle soluzioni a garanzia della propria tutela. In questo senso hanno integrato gli accordi con tali strumenti. Di conseguenza

> "[…] dal punto di vista dell'impresa, le soluzioni ora elencate comportino nuovi oneri organizzativi, che possono trovare giustificazione solo in un'ottica di medio o lungo periodo. A differenza del consenso dell'interessato, la scelta su quale fra le strategie in questione porre in essere richiede quindi una valutazione preliminare circa la natura, la complessità e la rilevanza dei flussi transfrontalieri che interessano l'impresa, nonché della continuità degli stessi nel tempo"[137].

Da una parte, dato il meccanismo di adesione sopra spiegato, le clausole possono essere interpretate come una manifestazione del consenso e della volontà consapevole e informata del trattamento e del trasferimento. Tuttavia, questa teoria è stata oggetto di non poche critiche da parte della dottrina. Le motivazioni si riconducono alla complessità dei trattamenti a cui i dati vengono sottoposti e di conseguenza alla difficoltà di fornire un'adeguata e comprensibile informativa all'interessato[138]. Essendo ancora oggi non pienamente trasparente la modalità con cui le agenzie di *intelligence* e le aziende operano sui dati personali degli utenti, sembra inverosimile che le parti contrattuali possano essere completamente e adeguatamente informate e, di conseguenza, che possano scegliere di aderire in maniera consapevole[139].

Dall'altra parte, la giurisprudenza delle sentenze *Schrems* ha ribadito che le clausole contrattuali tipo sono lo strumento giuridico che viene utilizzato maggiormente e reputato più sicuro al fine di tutelare il flusso di dati personali. Soprattutto nel caso in cui manchino gli accordi di adeguatezza a garantire l'esportazione dei dati verso Stati terzi. Infatti, al considerando n. 104 del GDPR, si ricorda che è fondamentale l'adozione di una decisione di

---

raggiungere un livello di protezione corrispondente allo stesso standard di «equivalenza sostanziale»".

[136] A. MANTELERO (2016: 248).

[137] Ivi, p. 253.

[138] J. TUROW, C. J. HOOFNAGLE, D. K. MULLIGAN, N. GOOD, J. GROSSKLAGS (2007: 723); R. M. CALO (2013: 1027 ss.); D. J. SOLOVE (2013: 1883); A. MANTELERO (2016: 250).

[139] A. MANTELERO (2016: 250).

adeguatezza per disciplinare determinati settori in Stati terzi, specificandone l'ambito di applicazione e il trattamento in suddetto territorio. Tuttavia, come ricordato all'art. 46, par. 2, lett. c), del GDPR, nel caso in cui mancasse una decisione di adeguatezza, le clausole contrattuali tipo risultano essere delle valide alternative. Infatti,

> "[a] tal proposito, l'articolo 46, paragrafo 1, del RGPD prevede che il titolare del trattamento può, in mancanza di una decisione di adeguatezza, trasferire dati personali verso un paese terzo «solo se ha fornito garanzie adeguate e a condizione che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi». Ai sensi dell'articolo 46, paragrafo 2, lettera c), del RGPD, tali garanzie possono risultare, in particolare, da clausole tipo di protezione elaborate dalla Commissione"[140].

Inoltre, si può specificare che la sicurezza delle clausole deriva dal fatto che queste vengono inizialmente negoziate tra l'importatore e l'esportatore e non sono poi modificabili. In questo senso, pongono in essere una vasta gamma di obblighi e di responsabilità nei confronti dell'importatore[141]. Inoltre, va ricordato che per quanto concerne la trattazione sulla privacy dei dati, le clausole tipo di protezione impongono dei vincoli direttamente nei confronti dell'importatore, ma nell'interesse del soggetto interessato che è beneficiario ultimo del contratto stipulato tra l'importatore e l'esportatore[142]. Nel caso in sentenza i beneficiari ultimi o soggetti terzi del contratto sono i cittadini dell'Unione europea. In questo senso si può dire che si manifesta una forma di "natura anticipatoria, nel senso che l'ordinamento comunitario si sostituisce all'autonomia dei privati"[143].

Al principio della non modifica delle clausole tipo di protezione viene fatta una deroga. Infatti, la decisione del 2010[144], all'art. 10, predispone una possibile modifica nel contratto nel caso in cui le parti si fossero impegnate a non modificare le clausole già presenti e a inserirne di nuove solo nella misura in cui non avessero contrastato con quelle già accordate nella decisione stessa[145]. Inoltre, ogni modifica delle clausole comporterebbe una revisione obbligatoria del testo modificato, da parte delle autorità garanti degli Stati interessati. Come da prassi, queste dovrebbero accettare e autorizzare il nuovo testo. Infatti, circa la modifica delle clausole si può evidenziare che

> "[…] da un lato la modifica delle clausole, nel caso in cui siano apprestate comunque garanzie adeguate o addirittura superiori (ad esempio, l'adozione di specifiche misure di sicurezze per la protezione dei dati) rispetto a quelle dettate dalla Commissione, risponde alle esigenze di tutela non solo delle controparti contrattuali, ma anche (e soprattutto) dei soggetti terzi (ossia dei soggetti cui

---

[140] Conclusioni dell'Avvocato generale Saugmandsgaard Øe *Schrems II*, punto 114.
[141] G. M. RICCIO (2016: 228).
[142] *Ibidem*.
[143] Ivi, p. 229.
[144] Esistono quattro tipi di decisioni modificative e integrative delle clausole tipo di protezione. In questo caso specifico si tratta della decisione 2010/87 della Commissione del 5 febbraio 2010.
[145] G. M. RICCIO (2016: 230).

> appartengono i dati personali). Dall'altro, se la variazione del testo delle clausole richiedesse l'autorizzazione preventiva dell'Autorità garante nazionale, allora sarebbe una soluzione in gran parte impraticabile, dal momento che causerebbe un significativo aumento dei tempi per l'approvazione del contratto e un aumento, altrettanto significativo, dei costi transattivi relativi al contratto stesso. La scarsa flessibilità delle standard contractual clauses, del resto, aveva indotto la Commissione ad adottare una Decisione nella quale, alle originarie clausole del 2001, erano affiancate clausole alternative e differenti, proposte e negoziate da un consorzio di associazioni imprenditoriali"[146].

In rimando alla sentenza, inizialmente il *Commissioner* ha considerato che le clausole di protezione tipo dei dati non fossero idonee a porre rimedio a una tutela carente. Infatti, in base a quanto verificato in prima ipotesi, le clausole conferivano agli interessati unicamente un tipo diritti contrattuali nei confronti dell'esportatore e dell'importatore dei dati, senza tuttavia vincolare le autorità di *intelligence* statunitensi[147]. Tuttavia, circa le questioni settima e undicesima che trattavano della validità della decisione 2010/87, viene ricordato infatti che

> "[l]'articolo 1 della decisione CPT dispone che le clausole tipo di protezione dei dati contenute nell'allegato della stessa decisione costituiscono garanzie sufficienti per la tutela della vita privata e della libertà e dei diritti fondamentali delle persone ai sensi dell'articolo 26, paragrafo 2, della direttiva 95/46. Quest'ultima disposizione è stata ripresa, in sostanza, all'articolo 46, paragrafo 1, e all'articolo 46, paragrafo 2, lettera c), del RGPD"[148].

Infatti, al punto 125 della sentenza viene detto che, benché la vincolatività delle clausole stipulate ponga degli obblighi in capo al titolare del trattamento e al destinatario del trasferimento, queste non possono vincolare le autorità dello stato in cui i dati vengono importati. Infatti, le autorità di tale paese terzo non sono parti del contratto stipulato tra importatore ed esportatore. Con riferimento a questo stesso punto, in sentenza si ricorda che

> "[…] è intrinseco al carattere contrattuale delle clausole tipo di protezione dei dati che queste ultime non possano vincolare le autorità pubbliche dei paesi terzi, e poiché tuttavia l'articolo 44, l'articolo 46, paragrafo 1, e l'articolo 46, paragrafo 2, lettera c), del RGPD, interpretati alla luce degli articoli 7, 8 e 47 della Carta, esigono che il livello di protezione delle persone fisiche garantito da tale regolamento non sia compromesso, può rivelarsi necessario completare le garanzie contenute in tali clausole tipo di protezione dei dati. A tal riguardo, il considerando 109 di tale regolamento enuncia che «[l]a possibilità che il titolare del trattamento (...) utilizzi clausole tipo di protezione dei dati adottate dalla Commissione (...) non dovrebbe precludere ai titolari del trattamento (...) di aggiungere altre clausole o garanzie supplementari» e precisa, in particolare, che questi ultimi «dovrebbero essere incoraggiati a fornire garanzie supplementari (...) che integrino le clausole tipo di protezione [dei dati]»"[149].

---

[146] G. M. RICCIO (2016: 230).
[147] Sentenza della Corte di giustizia *Schrems II*, punto 56.
[148] Ivi, punto 124.
[149] Ivi, punto 132.

Di conseguenza, in sentenza è stato stabilito che la decisione 2010/87 che istituisce le clausole, la c.d. decisione CPT,

> "[…] prevede meccanismi efficaci che consentono, in pratica, di garantire che il trasferimento verso un paese terzo di dati personali sulla base delle clausole tipo di protezione dei dati contenute nell'allegato di tale decisione sia sospeso o vietato qualora il destinatario del trasferimento non rispetti dette clausole o si trovi nell'impossibilità di rispettarle"[150].

Pertanto, alla luce della giurisprudenza della Corte e per le considerazioni di cui sopra, le clausole tipo di protezione sembrano ancora perdurare come mezzo di garanzia e protezione dei dati trasferiti in paesi terzi.

[150] Sentenza della Corte di giustizia *Schrems II*, punto 148.

Capitolo III

La tutela dei dati tra diritti fondamentali e libertà economiche: le nuove prospettive del consumatore

3.1 Gli articoli 7, 8 e 47 della Carta dei diritti fondamentali dell'Unione europea e il criterio di sostanziale equivalenza

La tematica del trasferimento dei dati verso Stati terzi apre a una molteplicità di interrogativi. Il primo che si rileva è la differenza che intercorre tra l'ordinamento statunitense e l'ordinamento europeo sul livello di tutela dei dati personali.

La decisione della Commissione che ha riconosciuto i principi del *Safe Harbor Agreement*, su cui poggia la pronuncia della Corte di giustizia circa la prima sentenza *Schrems*, risale al 26 luglio 2000. Ovvero, la decisione è pochi mesi antecedente alla proclamazione della Carta dei diritti fondamentali dell'Unione europea (Carta). Quest'ultima è stata promulgata la prima volta il 7 dicembre 2000 a Nizza e per questo è conosciuta anche come Carta di Nizza, sebbene successivamente adattata a Strasburgo dal Parlamento, dal Consiglio e dalla Commissione il 12 dicembre 2007.

Circa la Carta, il Trattato sull'Unione europea all'art. 6, par. 1, stabilisce che

> "[l']Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati"[151].

In questo senso la Carta assurge ad atto giuridicamente vincolante per le istituzioni europee e per gli Stati membri nel momento in cui questi applicano il diritto dell'Unione. Dunque, fin dal principio delle sentenze concernenti i dati, sembra che il portato della Carta abbia generato una sorta di "costituzionalizzazione"[152]. Infatti, a partire dalle sentenze *Digital Rights*

[151] L'art. 6 del Trattato sull'Unione europea (TUE) ai paragrafi successivi stabilisce che "[l]e disposizioni della Carta non estendono in alcun modo le competenze dell'Unione definite nei trattati. I diritti, le libertà e i principi della Carta sono interpretati in conformità delle disposizioni generali del titolo VII della Carta che disciplinano la sua interpretazione e applicazione e tenendo in debito conto le spiegazioni cui si fa riferimento nella Carta, che indicano le fonti di tali disposizioni". E che "2. L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati. 3. I diritti fondamentali, garantiti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali e risultanti dalle tradizioni costituzionali comuni agli Stati membri, fanno parte del diritto dell'Unione in quanto principi generali".

[152] O. POLLICINO, M. BASSINI (2016: 74).

Ireland[153] e *Google Spain*[154], sembra che la Corte di giustizia avesse cercato di compiere una riesamina di tutti quegli atti che sono entrati in vigore anteriormente alla Carta, cercando di dare uniformità al diritto dell'Unione in un'ottica di continuità tra i valori enunciati nella Carta e la giurisprudenza europea[155].

In questo senso, la tematica della raccolta e della conservazione dei dati assume una nuova prospettiva a partire dalla considerazione che in sentenza viene data agli articoli 7, 8 e 47 della Carta. Di conseguenza, si può dire che la Corte di Lussemburgo sia intervenuta nella prospettiva di estendere quanto più possibile la protezione dei dati personali e della privacy degli individui[156]. E lo ha fatto tentando di espandere la regolamentazione europea oltreoceano, tramite gli accordi di esportazione dei dati successivi al *Safe Harbor Agreement*, istituito dalla decisione 2000/520 e annullato con la sentenza *Schrems I*. Un primo tentativo di estensione delle garanzie è stato fatto sancendo la decisione 2010/87 sulle clausole tipo di protezione. Lo sforzo successivo è stato posto in essere con l'approvazione del *Privacy Shield* istituito dalla decisione 1250/2016, poi invalidata il 16 luglio 2020 con la sentenza *Schrems II*. E in ultimo, l'ampliamento delle garanzie è stato assicurato tramite il GDPR, il quale si occupa di regolamentare il trasferimento transfrontaliero dei dati a partire dall'art. 44.

Così, il disposto degli articoli della Carta ha una portata fondamentale. Infatti, l'interpretazione di entrambe le sentenze *Schrems* risulta essere una chiara conseguenza della lettura del quadro normativo fornito dagli articoli 7, 8 e 47 della Carta[157].

L'art. 7 della stessa Carta concerne il rispetto della vita privata e della vita familiare e stabilisce che "ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni"[158]. È bene sottolineare come il rispetto della vita privata e familiare sia un valore già sancito all'art. 8 della Convenzione europea dei diritti dell'uomo (CEDU)[159]. Questo infatti costituiva già una parte del

---

[153] Sentenza della Corte di giustizia dell'Unione europea dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland, Seitlinger e a.*

[154] Sentenza della Corte di giustizia dell'Unione europea del 13 maggio 2014, causa C-131/12, *Google Spain SL, Google Inc. c. Agencia Española de Protección de Datos e Mario Costeja Gonzàlez*.

[155] O. POLLICINO, M. BASSINI (2016: 75).

[156] *Ibidem.*

[157] F. ACCARDO (2017: 155 ss.).

[158] Art. 7 della Carta dei diritti fondamentali dell'Unione europea (CDFUE).

[159] La Convenzione europea dei diritti dell'uomo (CEDU), firmata dal Consiglio d'Europa nel 1950, è un trattato internazionale che ha l'obiettivo di tutelare i diritti umani e le libertà fondamentali in Europa. Tutti gli Stati membri del Consiglio d'Europa (47 Stati), di cui 27 sono gli Stati membri dell'Unione europea, sono segnatari della Convenzione. La convenzione ha istituito la Corte europea dei diritti dell'uomo, ente che supervisiona l'attuazione della Convenzione negli Stati membri. La Corte ha l'obiettivo di tutelare le persone dalle violazioni dei diritti umani. Ogni individuo i cui diritti siano stati violati, nell'ambito della Convenzione, da parte di uno Stato membro può rivolgersi alla Corte. Le sentenze hanno sempre il carattere

patrimonio comunitario, stando all'art. 6, par. 2, del TUE che stabilisce che "l'Unione [europea] aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali"[160]. L'art. 8 della CEDU sostiene anch'esso il diritto al rispetto della vita privata e familiare, prevedendo una deroga nel caso in cui la legge stabilisca delle misure di ingerenza che siano necessarie per la sicurezza nazionale, la sicurezza pubblica e il benessere economico. Ovvero, per difendere l'ordine e prevenire il crimine, o proteggere la salute, o la morale o, ancora, proteggere i diritti e le libertà degli altri. Altrimenti, come ribadito dallo stesso articolo, in una società democratica le istituzioni pubbliche non dovrebbero interferire nell'esercizio di questo diritto. L'articolo 8 stabilisce che

> "1. [o]gni persona ha diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza.
> 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui"[161].

L'art. 8 della Carta sulla protezione dei dati di carattere personale identifica il c.d. principio di lealtà, fondato sul consenso del trattamento da parte della persona interessata e il legittimo controllo da parte di autorità autonome sul rispetto di quanto disposto dall'articolo. Questo sancisce che

> "1. [o]gni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.
> 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.
> 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente"[162].

Ugualmente, l'art. 47 della Carta tutela l'individuo stabilendo il diritto a un ricorso effettivo e a un giudice imparziale. Infatti, quest'ultimo afferma che

> "[o]gni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni individuo ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni individuo ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese

---

di vincolatività e l'organo preposto a vigilare l'esecuzione di queste ultime è il comitato dei ministri del Consiglio d'Europa.

[160] Art. 6 del Trattato sull'Unione europea (TUE).

[161] Art. 8 della Convenzione europea dei diritti dell'uomo (CEDU).

[162] Art. 8 della Carta dei diritti fondamentali dell'Unione europea (CDFUE).

> dello Stato qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia"[163].

Il diritto dei cittadini a invocare un giudice a tutela delle salvaguardie è uno dei problemi da affrontare nei negoziati attualmente in corso tra l'Unione e altri Stati.

Questa valorizzazione degli articoli della Carta ha permesso alla Corte di giustizia di innalzare il controllo generale sul livello di protezione offerto dalla direttiva 95/46[164] e dalla decisione 2000/520. Infatti, il parametro di consenso per l'esportazione di dati personali al di fuori dall'Unione europea, è stato convertito da "adeguatezza", come indicato all'art. 25 della direttiva citata[165], a parametro di "sostanziale equivalenza", come espresso in diversi punti delle sentenze *Schrems*[166]. Inoltre, la stessa Corte ha sostenuto che la protezione dei dati personali dovesse essere valutata nell'ordinamento interno e nel campo del trasferimento verso Stati terzi "ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona" come già stabilito dalla direttiva e ribadito successivamente dalla Carta[167].

Già nella prima sentenza, la Corte ha avvalorato, seppur in maniera indiretta, uno sbilanciamento a favore di una tutela dei dati personali che si basasse su un criterio di equivalenza piuttosto che di adeguatezza[168]. Questo è emerso dalla lettura dell'art. 25 della direttiva 95/46 che si poneva l'obiettivo di "assicurare […] la continuità del livello elevato di tutela di tale protezione in caso di trasferimento di dati personali verso un paese terzo"[169]. In questo senso, il limite della continuità delle salvaguardie si è ritrovato nella differenza tra il significato di adeguatezza e il significato di sostanziale equivalenza[170]. Queste garanzie sono diventate la *conditio sine qua non* posta dalla Corte di giustizia per assicurare il trasferimento dei dati da un Paese ad un altro, allargando la prospettiva delle sentenze che guardava al trasferimento unicamente verso gli Stati Uniti.

---

[163] Art. 47 della Carta dei diritti fondamentali dell'Unione europea (CDFUE).
[164] Direttiva (CE) del Parlamento europeo e del Consiglio, del 24 ottobre 1995, 95/46, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.
[165] L'art. 25, par. 2, della direttiva 95/46/CE stabilisce che "[l']adeguatezza del livello di protezione garantito da un paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati; in particolare sono presi in considerazione la natura dei dati, le finalità del o dei trattamenti previsti, il paese d'origine e il paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate".
[166] Si faccia riferimento a quanto stabilito dalla sentenza *Schrems I* ai punti 74 e 96 e dalla sentenza *Schrems II* ai considerando n. 104 e ai punti 64, 65, 94, 96, 97, 105, 162, 178, 180, 181, 190, 191 e 193.
[167] O. POLLICINO, M. BASSINI (2016: 85).
[168] *Ibidem*.
[169] Direttiva (CE) del Parlamento europeo e del Consiglio, del 24 ottobre 1995, 95/46, *relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*.
[170] O. POLLICINO, M. BASSINI (2016: 85).

Così, trasformato il paradigma da adeguatezza a equivalenza, la Corte di Lussemburgo è giunta, in un primo momento, a invalidare la decisione che istituiva il *Safe Harbor Agreement* e, successivamente, la decisione di esecuzione istitutiva del *Privacy Shield*. Ed è proprio questo varco che è stato aperto dalla Carta ad aver dato un portato ancora più significativo alle sentenze. Infatti, sembra che lo stesso parametro di adeguatezza, inizialmente concepito come flessibile ed elastico, alla luce degli articoli 7, 8 e 47 della Carta fosse da interpretare in maniera rigida e definitiva[171].

Pertanto, da una parte, come ricordato anche dall'Avvocato generale nelle conclusioni *Schrems II*, è stato ammesso esplicitamente che la sostanziale equivalenza potesse essere assicurata, dagli Stati terzi, tramite strumenti diversi rispetto a quelli che venivano posti dall'Unione europea a garanzia della tutela dei dati personali[172]. Con l'unico limite che il livello di tutela proposto dovesse essere, nella sostanza, comparabile a quello posto in essere dall'Unione europea. In questo modo è stato ribadito che il fine ultimo dell'Unione fosse di assicurare una continuità delle salvaguardie, come sancito anche dagli agli articoli 45 e 46 del GDPR sui trasferimenti dei dati verso Stati terzi. Dall'altra parte, in questo modo la Corte di giustizia ha ammesso che si potesse pervenire ad un medesimo livello di tutela usando strumenti diversi di protezione. Di conseguenza, si potrebbe obiettare che almeno concettualmente la Corte ha ammesso che le norme a tutela dei dati personali adottate in ordinamenti differenti da quello dell'Unione europea fossero indiscutibili[173].

Tuttavia, la Corte ha certamente discusso gli strumenti normativi utilizzati dall'ordinamento statunitense. Nella seconda sentenza *Schrems* ha formalmente contestato la base giuridica dei programmi di sorveglianza PRISM e UPSTREAM, rintracciata nell'art. 702 del *Foreign Intelligence and Surveillance Act* e nell'*Executive order 12333*, citati in precedenza.

In vero, la Corte si è espressa in merito agli strumenti utilizzati dalle agenzie di *intelligence* statunitensi, reclamando che i diritti fondamentali dei cittadini europei fossero rispettati. In maggior misura, è proprio da questo intervento che prende avvio l'esame che la Corte svolge nelle sentenze *Schrems*. Si doveva appurare se le misure di tutela previste dagli accordi con gli Stati Uniti, prima dal *Safe Harbor Agreement* e poi dal *Privacy Shield*, collimassero a una tutela sostanzialmente equivalente.

Alla luce di quanto detto, sembra che la Carta abbia imposto una lettura rigorosa della tutela degli individui. In questo senso, l'indagine condotta dalla Corte di giustizia sulle garanzie previste negli Stati Uniti ha consentito di giudicare la sostanziale lontananza tra i due ordinamenti. Questo tipo di divergenza è pesata l'invalidità delle decisioni che stabilivano gli accordi sul trasferimento dei dati verso gli Stati Uniti. Infatti, la Corte di giustizia ha

---

[171] O. POLLICINO, M. BASSINI (2016: 85).

[172] Conclusioni dell'Avvocato generale Henrik Saugmandsgaard Øe del 19 dicembre 2019, causa C-311/2018, *Data Protection Commissioner contro Facebook Ireland Limited, Maximillian Schrems*, punto 118.

[173] O. POLLICINO, M. BASSINI (2016: 85).

verificato se ci fosse una conformità delle norme statunitensi a quelle europee circa la tutela dei diritti fondamentali, che venivano sintetizzati negli articoli 7, 8 e 47 della Carta, circa la tutela della vita privata e familiare, la tutela dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale, ovvero il diritto a un giusto processo.

Quindi, ci si è chiesto cosa fosse cambiato nel contesto giuridico tra la dichiarazione di adeguatezza degli accordi di trasferimento, del *Safe Harbor Agreement* nel 2000 e del *Privacy Shield* nel 2016, e la valutazione in direzione opposta con entrambe le sentenze *Schrems*.

Indubbiamente, per la prima sentenza, la nuova lettura del contesto giuridico si ritenne opportuna successivamente all'adozione della Carta, che entrò in vigore pochi mesi prima dalla decisione che istituì il *Safe Harbor Agreement*. Alla luce delle considerazioni compiute circa la sentenza *Schrems I* e se si guarda alla sentenza successiva in un'ottica di continuità della prima[174], il rapporto con la Carta racchiude l'elemento di continuità, assumendo un'importanza determinante. Ulteriormente a quest'ultima, nella sentenza *Schrems II* si immette il GDPR, entrato in vigore a decorrere dal 25 maggio 2018. In questo, fin dai primi considerando si denota un'evoluzione nella concezione dei dati personali. Tale evoluzione è stata declinata in senso di globalizzazione e, avvicinandosi all'ordinamento statunitense, di commercializzazione. Questo ha contribuito alla necessità di cambiare le prospettive europee e di dare una nuova lettura al sistema di trasferimento dei dati, pur mantenendo l'elevato livello di tutela come proposto dall'Unione fino ad ora.

In questo quadro, le sentenze *Schrems I* e *II* consentono di sopraggiungere alla conclusione che l'inadeguatezza degli accordi stilati tra l'Unione europea e gli Stati Uniti d'America emergesse da una lettura dei diritti incardinati agli articoli 7, 8 e 47 della Carta.

3.2 Gli individui tra *consumers* e *data subjects*

Dove vi è più distacco tra l'ordinamento statunitense e quello europeo è proprio sulle questioni centrali nella sentenza *Schrems II*, ovvero nel sistema di tutela del diritto alla riservatezza, nonché in materia di diritti azionabili e di accesso al giudice. Questo deriva dalle diverse concezioni che l'ordinamento europeo e quello statunitense hanno degli individui, intesi come *users*. Fanno riferimento, rispettivamente, alla nozione di *data subject*, ovvero di individuo identificabile tramite i dati, e a quella di *consumer*. Infatti, una delle questioni ancora aperte nel dibattito sul trasferimento transnazionale dei dati è sicuramente quella del concetto di consumatore.

La nozione economica di *consumer* validata dalle sentenze viene ora declinata in senso più globalizzato di quanto la si conoscesse prima[175]. È stato

[174] S. FANTIN (2020: 5).
[175] D. GUTIDRREZ COLOMINAS (2018: 542 ss.)

doveroso riconoscere, già a partire dai primi considerando del GDPR, l'estensione dei significati e del portato delle sentenze in cui sono centrali concetti come l'evoluzione tecnologica, la globalizzazione, la portata della condivisione.

La Corte di giustizia ha avuto quindi l'opportunità di definire cosa si intende per *consumer*. Basandosi sulla precedente giurisprudenza, la Corte ha affermato che una persona può essere considerata o meno un consumatore in base alla posizione che la persona interessata ricopre in un particolare contratto[176]. Infatti, lo scopo di un contratto viene considerato al di fuori del commercio o della professione di una persona se viene "concluso al fine di soddisfare i bisogni propri di individuo in termini di consumo privato"[177]. Sebbene secondo la Corte sussista quindi una distinzione tra i contratti conclusi a fini privati e quelli conclusi a fini professionali, la definizione di *consumer* si è rivelata difficile da applicare ai contratti che non rientrano chiaramente in una delle due categorie. Di conseguenza, i contratti relativi ai *social network*, come Facebook nelle sentenze, sono un esempio più che attuale di questo fenomeno[178]. Gli account *social* infatti vengono utilizzati per una molteplicità di scopi, talmente cangianti che rendono difficile identificare la linea di delimitazione tra l'uso pubblico e l'uso privato. Inoltre, il modo in cui questi account vengono utilizzati può cambiare significativamente nel tempo, pur permanendo ancora il contratto iniziale.

Inoltre, dall'altra parte si identifica l'individuo come *data subject*, laddove per *data subject* si intende

> "[…] any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"[179].

Pertanto, in base all'ordinamento e alle garanzie poste in capo agli utenti, si distinguono gli individui in *data subject*[180] e coloro che *data subject* non sono, ovvero a cui non sono garantite le tutele che provengono dal riconoscere un'identificazione tramite la raccolta e il *processing* dei dati personali. Ovvero, gli individui che rientrano nel paradigma di *consumers.*

In questo senso, in entrambe le sentenze *Schrems*, si ribadisce come l'ordinamento dell'Unione europea si ponga come risolutamente tutelante dei

---

176 T. LUTZI (2018: 374 ss.).
177 T. LUTZI (2018: 374 ss.) sostiene che: "[t]he purpose of a particular contract would only be considered to fall outside a person's trade or profession in the sense of Article 17(1) Brussels Ia if it were 'concluded for the purpose of satisfying an individual's own needs in terms of private consumption".
178 *Ibidem*.
179 Regolamento (UE) 2016/679, art. 4.
180 G. RESTA (2016: 39).

diritti dei cittadini, mentre quello statunitense faccia riferimento a una lettura dei cittadini come utenti-consumatori[181].

Alla luce di tali differenze, il GDPR propone una nuova lettura del cittadino-consumatore, nella prospettiva di un'integrazione economica e sociale[182]. Invero, la lettura in toto del GDPR fa comprendere come il concetto di globalizzazione sia legato alla nozione di tutela dei dati sempre stingente, così come proposta dall'Unione europea. Infatti, il considerando n. 7 del GDPR sancisce che

> "[t]ale evoluzione richiede un quadro più solido e coerente in materia di protezione dei dati nell'Unione, affiancato da efficaci misure di attuazione, data l'importanza di creare il clima di fiducia che consentirà lo sviluppo dell'economia digitale in tutto il mercato interno. È opportuno che le persone fisiche abbiano il controllo dei dati personali che li riguardano e che la certezza giuridica e operativa sia rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche"[183].

In questo senso, la privacy non appare solamente come schema normativo. Anzi, questa si profila sempre di più come il diritto ad avere diritti. In quest'ottica, i dati e il loro trattamento assumono una rilevanza anche da un punto di vista più politico ed economico. Infatti, la tutela dei dati personali è intesa come una delle linee di confine che definisce e distingue i sistemi democratici, assicurando che il trasferimento e l'accesso ai dati da parte di aziende private o di autorità pubbliche rispettino i principi di proporzionalità e necessità[184].

Tuttavia, il Relatore speciale delle Nazioni Unite per la privacy, Joseph Cannataci, ha sostenuto in un rapporto che fosse ironico come, tra tanti Stati che derivano i propri ordinamenti da una cultura giuridica più lontana dalla *Western legal tradition*[185], proprio gli Stati Uniti avessero ricevuto critiche per l'inadeguatezza delle garanzie poste a tutela degli *users*. Appartenendo a una cultura giuridica simile alla nostra, l'accordo con gli Stati Uniti avrebbe dovuto essere più facile, rispetto a quello con altri Stati. Peraltro, è bene ricordare che negli Stati Uniti la legislazione in materia di privacy è effettivamente disorganica e asimmetrica[186]. Infatti, vi è una sostanziale assenza del diritto alla tutela dei dati personali e, più in generale della privacy, nella legislazione dello Stato federale. In effetti, simili diritti vengono coperti in maniera marginale, indiretta e derivata dal diritto privato, passando per le norme che concernono, appunto, i consumatori[187]. Per tale motivo

---

[181] R. F. JØRGENSEN, T. DESAI (2017: 106 ss.).
[182] Regolamento (UE) 2016/679.
[183] *Ibidem*.
[184] P. PIRODDI (2016: 193).
[185] La *Western legal tradition*, in italiano letteralmente "tradizione giuridica occidentale", si riferisce appunto alle tradizioni giuridiche della cultura occidentale. Questa affonda le radici nel diritto sia nel diritto romano che nel diritto canonico. In questo senso si ricollegano cultura e sistemi giuridici.
[186] G. RESTA (2016: 36).
[187] *Ibidem*.

nell'ordinamento statunitense non si è proposto un paradigma degli *users* in accezioni diverse da quelle di *consumer*.

Infatti, lo stesso Relatore speciale ha ribadito, in un ulteriore rapporto, che

> "[t]he need to increase the control of individuals over their Internet privacy is being widely discussed. Individuals use their own devices and their data to obtain the information they require, such as maps and directions, and to view the advertisements they are interested in. In this regard, it is vital to ask, while technologies facilitating end-user control are important, to what extent can individuals exert sufficiently comprehensive protective control? The adoption of these tools conflicts with the economic forces currently shaping the Internet. Do governments have a role in the development and adoption of these tools?"[188].

Passando per le pronunce delle sentenze *Schrems I* e *II* si trova conferma del recupero dello spazio dei diritti fondamentali che concernono la tutela della privacy, sacrificando le libertà della sfera economica. Tanto che nella prima sentenza *Schrems* al punto 48, la Corte ha ammesso che la direttiva 95/46, che regolava il trasferimento di dati personali verso paesi terzi, riconosceva la necessità del trasferimento ai fini degli scambi commerciali[189]. Ciononostante, la Corte, allo stesso punto, ha posto un limite: i trasferimenti transfrontalieri dei dati potevano essere posti in essere solo alla presenza di un livello di protezione adeguato. Dunque, nonostante la Corte di giustizia avesse riconosciuto la necessità di esportare dati a scopi economici, le sentenze della stessa Corte sono propese per un'indiscussa e ribadita tutela degli individui, intesi come cittadini identificabili dai dati, piuttosto che come consumatori della rete.

In un'ottica di continuità con la giurisprudenza europea, le motivazioni commerciali non avrebbero potuto prevalere su quelle della privacy[190]. A partire dalla sentenza *Google Spain*, fino all'ultima *Schrems II*, è stato applicato un criterio di gerarchizzazione dei diritti fondamentali, dando priorità, in tal modo, alla protezione della privacy rispetto che all'interesse economico degli *internet service providers*[191]. La Corte, nelle sentenze non ha negato uno scopo commerciale del trasferimento dei dati, ma l'ha reso secondario a una tutela che è stata resa gerarchicamente primaria.

Così, partendo dalla decisione della Corte di giustizia dell'Unione europea nei casi *Schrems*, ci si può cioè soffermare sulle connessioni tra concorrenza, privacy e neutralità della rete in relazione ai flussi di dati transfrontalieri tra l'Unione e gli Stati Uniti d'America[192]. L'accumulo di

---

[188] Rapporto del Relatore speciale delle Nazioni Unite per il diritto alla privacy, del 19 ottobre 2017, A/72/540, *Big Data and Open Data interim report*, punto 108.

[189] O. POLLICINO, M. BASSINI (2016: 85).

[190] Ivi, p. 89 sostengono che "[c]osì, le ragioni del commercio non possono mai prevalere su quelle della privacy, se non in presenza di requisiti particolari. Sembra confermata la linea già intrapresa nella sentenza Google Spain, dove i diritti 'economici' soccombono rispetto alla privacy".

[191] G. GIANNONE CODIGLIONE (2016: 272).

[192] *Ibidem*.

informazioni personali da parte dei *social networks* sembrerebbe generare un nuovo tipo di surplus economico che potrebbe influenzare l'equilibrio del mercato, costruendo e rafforzando delle posizioni dominanti di monopolio di alcuni attori del web[193]. Di conseguenza, non è ingiustificata la posizione della Corte di giustizia nelle sentenze *Schrems I* e *II*. Nell'era dei *big-data*, è necessario promuovere la protezione e la tutela dei dati, cercando di assicurare una concreta convergenza tra le regole anti-monopolistiche dell'economia di internet e la privacy, nel quadro di un'efficace applicazione dei diritti fondamentali[194].

Dal lato del mercato, sul binomio privacy individuale e mercati, i dati devono essere considerati come "beni economici, scambiabili liberamente tra imprese e necessari a promuovere lo sviluppo del commercio internazionale"[195]. E che

> "[n]egli ultimi anni, il regime di utilizzo dei dati da parte dei prestatori ha superato la mera funzione di volano delle strategie commerciali (si pensi alle preferenze d'acquisto desumibili dal c.d. profiling e alle proposte individuali effettuabili attraverso il behavioural advertising): sono i dati stessi l'oggetto principale dell'attività imprenditoriale. Il dato – sia personale che anonimo – viene captato, veicolato, trattato e nella maggior parte conservato ed accumulato, rappresentando una forma di capitale diverso e alternativo al plusvalore ottenuto dalla vendita dei servizi o degli spazi pubblicitari"[196].

Infatti, dal lato più economico, è stato tentato di determinare un punto di convergenza tra la tutela dei dati nel loro trasferimento e il loro utilizzo in un contesto economico. Un passo in questa direzione è stato l'approvazione della decisione 2010/87 sulle clausole contrattuali tipo. Questa, anche in seguito alla sentenza *Schrems II*, è rimasta immodificata, ammettendo così la possibilità di una commercializzazione dei dati. Le clausole contrattuali sono, in questo senso, dei contratti e si applicano all'esportazione dei dati in tutti gli Stati che le siglano con l'Unione europea[197]. Infatti, delle ricerche illustrano come il flusso dei dati tra Unione europea e Stati terzi si stabilisca sulle clausole, intese come canale preferenziale per il trasferimento.

Uno studio intitolato *Schrems II: Impact Survey Report*, del novembre 2020, indica che oltre trequarti delle aziende europee utilizzano clausole di protezione tipo per trasferimenti verso più di un paese non europeo[198]. Solo il 9% degli intervistati non trasferisce dati al di fuori dall'Unione e il 5% usa altri meccanismi di trasferimento. Inoltre, lo studio ha dimostrato che quasi la totalità delle aziende prese in analisi trasferiscono dati verso gli Stati Uniti. Quasi il 60% delle aziende esporta dati in Asia e Regno Unito. Lo studio ha evidenziato che le aziende europee che trasferiscono dati diretti in Medio

---

[193] G. GIANNONE CODIGLIONE (2016: 271).
[194] Ivi, p. 304.
[195] Ivi, p. 273.
[196] *Ibidem*.
[197] Decisione 2010/87.
[198] Studio di DigitalEurope, BusinessEurope, ERT e ACEA, del novembre 2020, *Schrems II: Impact Survey Report*.

Oriente e Africa sono meno, circa il 18% e ancora meno quelle che esportano verso il Sudamerica, pari a circa il 10%[199].

Inoltre, secondo quanto riportato in uno studio del 2020 della Commissione europea, intitolato *The European data market study update*, è previsto che l'economia dei dati dell'Unione europea crescerà all'ammontare di 827 miliardi di euro entro il 2025. Nonché, che la ripresa dell'economia europea dopo la crisi Covid sarà affidata proprio alla capacità di trasferire dati oltre le frontiere europee[200].

Di conseguenza, sembra inevitabile negare un utilizzo economico dei dati personali dei cittadini dell'Unione europea, nonostante nelle sentenze *Schrems* si sia dato un rilievo primario alla tutela prima che alla commercializzazione. Quest'ultima si può ammettere solamente alla stregua di garanzie che l'Unione europea reputa non negoziabili.

[199] Studio di DigitalEurope, BusinessEurope, ERT e ACEA, del novembre 2020, Schrems *II: Impact Survey Report*.

[200] Final study report D2.9 della Commissione europea, 2020, *The European data market monitoring tool: key facts & figures, first policy conclusions, data landscape and quantified stories*, p. 28 ss.

Conclusioni

La tutela del trattamento dei dati personali è una materia in continua evoluzione nella giurisprudenza europea. È stato evidenziato come vi sia una lontananza non indifferente tra i diversi ordinamenti normativi circa il tema della tutela dei dati personali. Gli Stati Uniti d'America adottano una logica fondata essenzialmente su una patrimonializzazione dei dati personali in un contesto neoliberista. Quest'ultima concezione si è scontrata con la dottrina europea che afferma che i diritti fondamentali sono di rango sovraordinato rispetto ad altri diritti fondamentali che si possono basare sulla patrimonializzazione e commercializzazione. Per l'evoluzione e la grandezza degli *internet service providers* come Facebook e Google si può dire quasi scontato che la posizione preminente fosse quella di una commercializzazione dei dati. Tuttavia, la portata delle sentenze della Corte di giustizia che sono state emanate in questi anni a tale proposito ha dato risposte nettamente in contrasto con la disciplina statunitense.

Tuttavia, è stato trovato un punto di contatto tra le concezioni, in quanto entrambe fanno capo ad una base identificabile come *western legal tradition*. Pertanto, nella sostanza ci si confronta con dei modelli in cui le ingerenze dovrebbero avvenire unicamente per motivi di sicurezza. In questo senso, il monito delle sentenze *Schrems I* e *II* è di prestare attenzione che sotto il motivo di sicurezza non si nasconda il pretesto per una raccolta indiscriminata.

Come rilevato, dove vi è più distacco tra i due ordinamenti è proprio sulla questione al centro della sentenza *Schrems II*: nel sistema di tutela del diritto alla riservatezza, in materia di diritti azionabili e di accesso al giudice. Il sistema statunitense distingue infatti i cittadini americani e i cittadini di Stati terzi. Questo nel mondo "dematerializzato" dei dati pone un problema di non poco conto, un conflitto con la posizione della Corte di giustizia dell'Unione europea, ovvero di principi e diritti riconosciuti a tutti, indistintamente. Il fatto che esista questa differenza di trattamento nell'invocare le salvaguardie è uno dei problemi da affrontare nei negoziati.

Inoltre, circa la distanza sulla concezione di *consumer*, si può dire che questa sia stata parzialmente accettata dall'Unione. Infatti, se è vero che la sentenza *Schrems II* ha eliminato il *Privacy Shield* come strumento legale specifico per regolare gli scambi transatlantici, è anche vero che ha creato il presupposto per un flusso di dati con altri Paesi. Questi diventano in questo modo dei partner economici, forgiando una situazione relativamente nuova anche per l'Unione europea, la cui sfida sarà trovare l'equilibrio del binomio tutela-commercio dei dati personali.

La soluzione a cui ricorrere in questo senso dovrebbe essere globale. Ovviamente con le dovute cautele, in quanto negli Stati Uniti la legislazione in materia di privacy è appena emergente. Infatti, vi è una sostanziale assenza nel diritto federale della tutela della privacy.

Tramite il GDPR l'Unione europea ha effettuato il tentativo di regolamentare siffatti trasferimenti. Ai sensi dell'art. 44 del GDPR si disciplinano tutti i trasferimenti di dati all'estero, ovvero al di fuori delle frontiere

dell'Unione. Come regolato agli articoli successivi, per tutelare il trasferimento andrebbero compiuti accertamenti e valutazioni di adeguatezza per tutti i dati esportati verso Stati terzi, fatti salvi i Paesi con cui l'Unione europea ha stipulato degli accordi *ad hoc*[201].

Attualmente, la reazione a *Schrems II* ha rafforzato il lavoro in tema di adeguatezza, stilando nuove regole e concludendo accordi con Paesi terzi, implementando l'uso di clausole tipo di protezione. Così, la pronuncia della Corte non ha riguardato solamente gli Stati Uniti d'America e non interessa solo le società del digitale o la *silicon valley*. Quindi, nonostante le valutazioni compiute caso per caso, si sta lavorando per dare attuazione alla sentenza *Schrems II* con le nuove clausole contrattuali standard che dovranno dare concretezza alla sentenza in modo uniforme e armonizzato, per aiutare le società che non hanno le risorse per svolgere l'analisi comparatistica richiesta dall'ultima sentenza.

In definitiva, si può dire che questa seconda sentenza *Schrems* abbia una portata di sistema per quanto concerne i trasferimenti transfrontalieri dei dati.

[201] Al considerando n. 102 del GDPR viene stabilito che "[i]l presente regolamento lascia impregiudicate le disposizioni degli accordi internazionali conclusi tra l'Unione e i paesi terzi che disciplinano il trasferimento di dati personali, comprese adeguate garanzie per gli interessati. Gli Stati membri possono concludere accordi internazionali che implicano il trasferimento di dati personali verso paesi terzi o organizzazioni internazionali, purché tali accordi non incidano sul presente regolamento o su qualsiasi altra disposizione del diritto dell'Unione e includano un adeguato livello di protezione per i diritti fondamentali degli interessati".

Bibliografia

ACCARDO (2017), *L'invalidità del Safe Harbor Agreement*, in *Ricerche giuridiche*, p. 155 ss.

BRADFORD (2020), *The Brussels Effect: How the European Union Rules the World*, Oxford.

CALO (2013), *Against Notice Skepticism in Privacy (and Elsewhere)*, in *Notre Dame Law Review*, p. 1027 ss.

CRESPI (2015), *La tutela dei dati personali UE a seguito della sentenza Schrems*, in *Eurojus*, reperibile *online*.

CRESPI (2016), *Il trasferimento dei dati personali UE in Stati terzi: dall'approdo sicuro allo Scudo UE/USA per la privacy*, in *Diritto pubblico comparato ed europeo*, p. 687 ss.

F. ROSSI DAL POZZO (2016), *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona. (Dal Safe Harbour al Privacy Shield)*, in *Rivista di diritto internazionale*, p. 721 ss.

FANTIN (2020), *Data Protection Commissioner v Facebook Ireland Limited, Maximillian Schrems: AG discusses the validity of standard contractual clauses and raises concerns over privacy shield*, in *European data protection law review: EDPL*, p. 325 ss.

FOSSÀ (2017), *Facebook nel mirino delle Corti: accanimento giurisprudenziale a cavallo del caso Schrems?*, in *Ricerche giuridiche*, p. 103 ss.

GIANNONE CODIGLIONE (2016), *Libertà d'impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 271 ss.

GIATTINI (2016), *La tutela dei dati personali davanti alla Corte di giustizia dell'UE: il caso "Schrems" e l'invalidità del sistema di 'approdo sicuro'*, in *Diritti umani e diritto internazionale*, p. 247 ss.

GUTIÉRREZ COLOMINAS (2018), S*chrems v Facebook: the consumer definition in the framework of digital social networks*, in *European data protection law review: EDPL*, p. 542 ss.

HOFFMAN (2015), *On the Schrems Decision*, in *Europaeus, EU law and policy*, reperibile *online*.

JAULT-SESEKE, ZOLYNSKI (2016), *Le règlement 2016/679/UE relatif aux données personnelles*, in *Recueil Dalloz*, p. 1878 ss.

JØRGENSEN, DESAI (2017), *Right to Privacy meets Online Platforms: Exploring Privacy Complaints against Facebook and Google*, in *Nordic journal of human rights*, p. 106 ss.

KUNER (2012), *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, in *BNA Bloomberg Privacy and Security Law Report*, p. 215 ss.

LUTZI (2018), *"What's a consumer?": (some) clarification on consumer jurisdiction, social-media accounts, and collective redress under the Brussels Ia Regulation: case C-498/16 Maximilian Schrems v. Facebook Ireland Limited*, in *Maastricht journal of European and comparative law: MJ*, p. 374 ss.

M. SCHREMS (2016), *The Privacy Shield is a Soft Update of the Safe Habor*, in *European Data Protection Law Review: EDPL*, p. 148 ss.

MANTELERO (2016:), *I flussi di dati transfrontalieri e le scelte delle imprese tra Safe Harbour e Privacy Shield*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 239 ss.

MONTI, WACKS (2019), *Protecting personal information: the right to privacy reconsidered*, Oxford.

NINO (2013), *Il caso Datagate: i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti umani e diritto internazionale*, p. 727 ss.

NINO (2015), *La corte di giustizia UE dichiara l'invalidità del sistema di Safe Harbour: la sentenza Schrems*, in *SIDIBlog*, reperibile *online*.

PIRODDI (2016), *I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 169 ss.

POLLICINO, BASSINI (2016), *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 73 ss.

RESTA (2016), *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 23 ss.

RICCIO (2016), *Model Contract Clauses e Corporate Binding Rules: valide alternative al Safe Harbor Agreement?*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 215 ss.

SICA, D'ANTONIO (2016), *Verso il Privacy Shield: il tramonto dei Safe Harbour Privacy Principles*, in RESTA et al. (a cura di), *La protezione transnazionale dei dati personali: dai "Safe Habour Principles" al "Privacy Shield"*, Roma, p. 137 ss.

SOLOVE (2013), *Introduction: Privacy Self-management and The Consent Dilemma*, in *Harvard Law Review*, p. 1883 ss.

STANZIONE (2016), *Il nuovo regolamento europeo sulla protezione dei dati personali: genesi ed ambito di applicazione*, in SICA et al. (a cura di), *La nuova disciplina europea della privacy*, Padova, p. 30 ss.

TUROW, HOOFNAGLE, MULLIGAN, GOOD, GROSSKLAGS (2007), *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, in *I/S: A Journal of Law and Policy for the Information Society*, p. 723 ss.

The cross-border transfer of personal data: the privacy protection in the European Union in the light of the *Schrems II* judgment.

The data protection is an evolving subject in the European jurisprudence. In particular the judgments concerning the events involving Facebook and Google have affirmed that it is one of the cornerstones of the European Union. When we refer to the *Schrems I and II* judgments, we are talking about the group of judgments that describe the position of European case law on the subject of cross-border data transfers. Both judgments are named after an Austrian citizen, that is called Maximilian Schrems, who raised them in several fora. He repetitively pointed out that the US law did not provide data subjects, identified whit the users of the social network Facebook, with a level of data protection comparable to the data protection provided by the European law.

The first judgment, remembered *as Schrems I*, refers to the ruling of the Court of Justice of the European Union (CJEU) in Case C-362/14, *Maximilian Schrems v. Data Protection Commissioner*. The second judgment is in continuity with the first, as if it were a "second stage". It is referred to the CJEU's ruling on Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems*. However, since the concluding judgment of 16 July 2020 the perspective is broadened, even if it starts from a dispute about the processing of personal data of EU citizens in the US. In this perspective, it can be seen what the so-called Brussels effect is. It refers to a regulatory globalisation of the European Union that externalises its law beyond its borders. In general, it is no longer only the United States that is looked at.

The outcome of the first judgment marks the transition from the Safe Harbor Agreement, that is a "primitive" cross-border transfer system, to an apparently more protective system, the Privacy Shield. The second judgment invalidates the latter, describing a new protection of citizens and their data within the European Union and in relations with third parties. *Schrems II* integrates the subject of protection with innovative visions that have been reinforced in the European jurisprudential debate. It is therefore necessary to retrace the stages of the legislation that led to this latest judgment.

The transfer of data to third countries was formally governed by Decision 2010/87/EU on the initiation of standard contractual clauses, identified as "sufficient guarantees for the protection of the privacy and fundamental rights and freedoms of individuals".

The scandal emerged from a report published by a US computer scientist, Edward Snowden, on the activities of the US intelligence services and the operations of the National Security Agency (NSA). It thus highlighted the ineffectiveness of the previous system, the so-called Safe Harbor Agreement, highlighting its limits and calling for an evolution of personal data protection.

Hence, the conclusion of the first judgment is that

> "1. [a]rticle 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data as amended by Regulation (EC) No 1882/2003 of the European Parliament and of the

> Council of 29 September 2003, read in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights of the European Union, must be interpreted as meaning that a decision adopted pursuant to that provision, such as Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State, within the meaning of Article 28 of that directive as amended, from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection.
> 2. Decision 2000/520 is invalid".

Following the conclusions of AG, it can be argued that the decision was intended to allow the flow of data between the European Union and the United States. However, it should have provided for adequate protection of citizens' data, as required by EU law. It is in this direction that European case-law is progressing, thanks to the Schrems I judgment and the move towards other more advanced data protection systems in line with developments in the field. The first stage was marked by the EU-US Privacy Shield and the General Data Protection Regulation.

The Privacy Shield was strongly criticised for not sufficiently binding US companies and authorities to comply with their agreements with the EU. Maximilian Schrems himself called it a "soft update of Safe Harbour [Agreement]". On the other hand, the GDPR ensures a higher level of protection, also thanks to standard protection clauses.

The GDPR itself, in its first recitals, refers precisely to the concept of globalisation and the need for data transfer, which is increasingly the manifestation of a new trade, a network of economic relations. In fact, it is precisely in this sense that the *Schrems* judgments assume significant importance. It is stated in *Schrems I* and reiterated in *Schrems II* that, in the event of data being transferred abroad, continuity of safeguards must be ensured. In both judgments, this continuity of securities is defined as "substantial equivalence". This can be achieved by different tools but must consist of a final result that is at least comparable in terms of protection. According to the CJEU and the AG in both *Schrems* judgments, a continuity of protection must be ensured which extends beyond the borders of the European Union. This "substantial equivalence" can also be ensured by different means than those used by the Union, but the equivalence must be found in the final result. This should be a comparable level of protection.

The protection of the personal data is a subject that is evolving in the European jurisprudence. The judgments involving Facebook and Google have affirmed that it is now one of the cornerstones of the European Union. It is covered by Articles 7, 8 and 47 in the Charter of Fundamental Rights of the European Union (also known as Charter). The evolution has been marked and regulated most recently by the GDPR. Article 4 of the GDPR contains

definitions that help us understand what is meant by personal data, data processing and cross-border processing. Articles 44, 45 and 46 of the GDPR describe what is meant by cross-border transfer and how it is to be regulated. Indeed, in both *Schrems* judgments reference is made to a flow of personal data between the European Union and the United States of America. Already since Article 44 of the GDPR, the transfer takes on a general scope with regard to third states importing data from the EU. In fact, the new regulation fits in between the two judgements, leading to a reinterpretation of the regulatory context.

The Article 44 states that

> "[a]ny transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined".

And this article substantially opens up the regulation of data transfer. Under Article 44 of the GDPR, all data transfers outside the borders of the Union are regulated. As stated in the following articles, in order to protect the transfer, assessments and adequacy evaluations should be carried out for all data exported to third countries, with the exception of countries with which the EU has concluded ad hoc agreements.

The issue of the transfer of data to non-EU countries has raised a number of questions. First of all, it has revealed the difference between US and European law on the level of protection of personal data. Also, what is the different conception of data subjects and consumers derives from these different readings and different interpretations of the digital evolution. These are the issues at the heart of the *Schrems II* judgment, which go beyond the transatlantic relationship, extending the need for protection.

Within EU law, the judgments are an expression of a convergence movement in the world of privacy. Several jurisdictions are adopting privacy frameworks that are based on similar substantive principles or governance mechanisms, such as the establishment of independent supervisory authorities. This is a global trend involving California, Japan – with which one of the largest data exchange zones has been created for non-identical but common principles – Brazil, Korea and Indonesia. These common guarantees can ensure data protection and data transfers. They are the *conditio sine qua non* set by the CJEU to ensure the transfer.

In this sense, privacy is not just a regulatory scheme. Data and their processing are also relevant from a more political and economic point of view. Privacy is increasingly understood as one of the boundary lines that define and distinguish democratic systems. According to the system and the guarantees placed on them, the citizens of states are distinguished into data subjects

and consumers. In other words, privacy is increasingly emerging as the right to have rights. Ensuring that the transfer and access to data by private companies or public authorities respect the principles of proportionality and necessity. These are the issues of the *Schrems II* judgment, which go beyond the transatlantic relationship.

The protection of the processing of personal data is an evolving subject in European case law. It has been pointed out that there is a considerable gap between the different legal systems on the subject of personal data protection. The United States of America adopts a logic based essentially on the patrimonialisation of personal data in a neo-liberal context. This latter conception has conflicted with European doctrine, which affirms that fundamental rights are of a higher rank than other fundamental rights that are based on patrimonialisation and commercialisation. Due to the evolution and size of internet service providers such as Facebook and Google, it can almost be taken for granted that the pre-eminent position was that of data commercialisation. However, the scope of the judgments of the CJEU that have been handed down in this respect in recent years has given answers that are clearly at odds with the US rules.

Nevertheless, a point of contact has been found between the two concepts, since they both refer to a basis that can be identified as the Western legal tradition. In essence, therefore, one is confronted with models in which interference should only take place for security reasons. In this sense, the warning of the *Schrems I and II* judgments is to be careful that the security reason does not hide the pretext for indiscriminate collection.

As noted, where there is the greatest gap between the two systems is precisely on the issue at the heart of the *Schrems II* judgment: in the protection of the right to privacy, in the matter of enforceable rights and access to the courts. The right of citizens to invoke a court to protect their safeguards is one of the issues to be addressed in the current negotiations between the Union and other states.

Moreover, as regards the distance on the concept of consumer, it can be said that this has been partially accepted by the Union. In fact, if it is true that the *Schrems II* judgment has eliminated the Privacy Shield as a specific legal instrument to regulate transatlantic trade, it is also true that it has created the conditions for a flow of data with other countries. These countries thus become economic partners, forging a relatively new situation also for the European Union, whose challenge will be to balance the protection-trade combination of personal data.

The issue of data transfer to third countries raises a number of questions. The first question to be asked is the difference between US and European law on the level of protection of personal data. The solution to be used in this respect should be a global one. With due caution, as in the US, privacy legislation is barely emerging. In fact, there is a substantial absence of privacy protection in federal law.

Through the GDPR, the European Union has made an attempt to regulate such transfers in a global way. Under Article 44 of the GDPR, all data

transfers abroad, i.e. outside the borders of the Union, are regulated. As regulated in the subsequent articles, adequacy assessments and evaluations should be carried out for all data exported to third countries, with the exception of countries with which the EU has concluded *ad hoc* agreements, in order to protect the transfer.

Currently, the reaction to *Schrems II* has strengthened the work on adequacy by drafting new rules and concluding agreements with third countries, implementing the use of standard protection clauses. Thus, the CJEU's ruling did not only concern the United States of America and does not only affect digital companies or Silicon Valley. Therefore, despite the case-by-case evaluations, work is underway to implement the Schrems II ruling with the new standard contractual clauses that will have to give substance to the ruling in a uniform and harmonised manner, to help companies that do not have the resources to carry out the comparative analysis required by the latest ruling. Ultimately, this second *Schrems II* judgment can be said to have a systemic scope with regard to cross-border data transfers.

Consequently, the CJEU can be said to have intervened with a view to extending the protection of personal data and the privacy of individuals as far as possible. Already in the first *Schrems* judgment, the CJEU indirectly confirmed an imbalance in favour of personal data protection based on an equivalence rather than an adequacy criterion.

In accordance with the above, it seems that the Charter has imposed a strict reading of the protection of individuals. In this sense, the survey carried out by the CJEU on the guarantees provided for in the United States made it possible to judge the substantial divergence between the two systems. This kind of divergence weighed against the invalidity of the decisions establishing the agreements on the transfer of data to the United States. Indeed, the CJEU examined whether there was a conformity of the US rules with the European rules on the protection of fundamental rights, which were summarised in Articles 7, 8 and 47 of the Charter, concerning the protection of private and family life, the protection of personal data and the right to an effective remedy and to a fair trial.

In the light of these differences, the GDPR proposes a new reading of the citizen-consumer, in the perspective of economic and social integration. Indeed, reading the GDPR in its entirety shows how the concept of globalisation is linked to the notion of data protection that is always stinging, as proposed by the European Union.

In addition, the economic notion of consumer validated by the judgments is now declined in a more globalised sense than was previously known. It was necessary to recognise, already from the first recitals of the GDPR, the extension of the meanings and the scope of the judgments in which concepts such as technological evolution, globalisation and the scope of sharing are central. Therefore, on the basis of the system and the guarantees placed on users, a distinction is made between individuals who are data subjects and those who are not data subjects, i.e. who are not guaranteed the protections that come from recognising an identification through the collection and

processing of personal data. That is, individuals who fall under the paradigm of consumers.

Hence, this thesis emphasised that the European Union has never established a relationship of exclusion between data protection and data commercialisation. In the light of these judgments, the CJEU's position has been of integration between the two concepts. The result was that data protection in the European Union remains the central and non-negotiable objective.