ISSN 1826-3534

federalismi.it
RIVISTA DI DIRITTO PUBBLICO ITALIANO, COMPARATO, EUROPEO

15 GIUGNO 2022

Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard

di Chiara Bertoldi
Dottoranda di ricerca in Diritto costituzionale ed europeo
Università del Piemonte Orientale

Tutela dei diritti e accesso ai dati personali da parte delle autorità governative: l'equilibrio precario della decisione di adeguatezza e delle clausole contrattuali standard*

di Chiara Bertoldi
Dottoranda di ricerca in Diritto costituzionale ed europeo
Università del Piemonte Orientale

Abstract [It]: Il funzionamento delle basi giuridiche che legittimano il trasferimento transfrontaliero di dati verso Stati terzi è stato messo a dura prova dall'accesso ai dati da parte delle autorità governative di questi ultimi. Il contributo ha lo scopo di effettuare, alla luce delle sentenze *Schrems I* e *Schrems II*, una disamina delle modifiche legislative e di prassi intervenute in merito alla decisione di adeguatezza e alle clausole contrattuali standard con specifico riferimento al tema dell'accesso ai dati da parte delle autorità governative. Verrà infine analizzata la nuova decisione della Commissione sulle clausole contrattuali tipo e come questa cerchi di offrire una maggiore tutela nei confronti dell'interessato a fronte dell'intrusione, nei propri diritti, da parte delle autorità pubbliche degli Stati destinatari dei dati.

Title: Protection of rights and access to personal data by government authorities: the unstable balance of the adequacy decision and standard contractual clauses
Abstract [En]: The functioning of the legal bases legitimising cross-border data transfer to third Countries has been severely challenged by the access to data by government authorities of such Countries. In the light of the *Schrems I* and *Schrems II* judgments, this contribution aims at analysing the changes in law and practice concerning adequacy decision and standard contractual clauses with specific reference to the issue of access to data by government authorities. Finally, it will be analysed the new Commission decision on standard contractual clauses and how it seeks to offer greater protection to data subjects against the intrusion of their rights by the public authorities of the States receiving the data.

Parole chiave: dati personali, trasferimenti transfrontalieri, autorità governative, clausole contrattuali standard, decisione di adeguatezza
Keywords: personal data, cross-border transfers, government authorities, standard contractual clauses, adequacy decision

* Articolo sottoposto a referaggio.

1. Introduzione

In un mercato sempre più dipendente dal processo di digitalizzazione, il flusso di dati a livello globale costituisce il mezzo di sviluppo principale delle relazioni commerciali ed economiche tra Stati. Tale processo di digitalizzazione, oltre a promuovere la concorrenza tra aziende e ridurne i costi, genera un incremento notevole nella fornitura di beni e servizi. Le piattaforme digitali che operano nell'ambito della comunicazione e dell'*electronic commerce* rappresentano punti di snodo che facilitano gli scambi economici e, per funzionare correttamente, non possono prescindere dal flusso di dati. Il flusso transnazionale di dati ha assunto un ruolo di spiccato rilievo all'interno del mercato globale, tanto da essere definito come «*commerce-enabling «hallmarks of 21st century globalization» and «the connective tissue holding the global economy together»*»[1]. I flussi di dati consentono, infatti, non solo di trasmettere aggregati di informazioni di qualsiasi tipo ma anche di garantire il transito di persone, servizi, beni e capitali, tanto da essere considerati come fonti di valore economico maggiori del tradizionale commercio dei beni[2]. La crescita delle imprese che operano nell'ambito dell'economia digitale è strettamente dipendente dalla capacità di trasferire i dati. I trasferimenti di dati non sono solo un aspetto chiave del commercio internazionale ma sono cruciali per lo sviluppo economico in senso ampio. Secondo lo studio condotto nel giugno 2021 da *Digitaleurope*, circa la metà del PIL dell'Unione proviene da settori che ruotano attorno al trattamento dei dati[3].

Se, da un lato, il trasferimento di dati, che consente la creazione di archivi digitali contenenti informazioni su milioni di utenti, costituisce il motore della nuova economia globale, dall'altro, solleva numerosi interrogativi sul rispetto di diritti fondamentali, quali il diritto alla riservatezza, il diritto alla *privacy*, il diritto all'oblio e il diritto all'autodeterminazione[4].

Ci troviamo di fronte a un fenomeno senza precedenti e, nonostante la raccolta, il trattamento e il trasferimento dei dati siano, in seguito agli scandali dell'ultimo decennio, al centro dell'attenzione della contemporaneità non solo giuridica, fatta eccezione per una serie di pubblicazione nell'ambito del diritto commerciale o del diritto privato internazionale, il diritto internazionale pubblico risulta carente in materia. Le ragioni di questa carenza risiedono nella qualità rivestita dai soggetti che nel cyberspazio operano maggiormente che, pur essendo spesso multinazionali, rimangono pur sempre attori privati e non pubblici[5]. È in questo complesso ecosistema giuridico-digitale che si colloca l'Unione europea.

[1] W. G. VOSS, *Cross-Border Data Flows, the GDPR, and Data Governance*, in *Washington International Law Journal*, n. 3, 2020, p. 487.
[2] J. MANYIKA, S. LUND, J. BUGHIN, J. WOETZEL, K. STAMENOV, D. DHINGRA, *Digital Globalization: The New Era of Global Flows*, in *McKinsey Global Institute*, 2016, pp. 23 ss.
[3] Lo studio condotto da *Digitaleurope* è consultabile alla pagina Data Flows and the Digital Decade.
[4] S. B. PAN, *Get to Know Me: Protecting Privacy and Autonomy under Big Data's Penetration Gaze*, in *Harvard Journal of Law & Technology*, n. 1, 2016, pp. 239 ss.
[5] G. DELLA MORTE, *Big Data e Protezione Internazionale dei Diritti Umani. Regole e Conflitti*, Editoriale Scientifica, Napoli, 2018, p. 6.

L'obiettivo dell'Unione in materia è duplice. Da un lato, garantire la libera circolazione dei dati personali e, dall'altro, assicurare la tutela dei dati personali sia durante il loro trattamento che durante il loro trasferimento. L'art. 16 del Trattato sul Funzionamento dell'Unione europea (TFUE) sancisce il dovere delle istituzioni di predisporre norme relative sia alla tutela dei dati delle persone fisiche oggetto di trattamento che alla libera circolazione dei dati[6]. Tuttavia, il mantenimento del delicato bilanciamento degli obiettivi posti dall'Unione non è affatto semplice. Opportunità di *partenership* commerciali con Stati terzi possono portare all'abbassamento delle garanzie di protezione dei dati, liberalizzandone conseguentemente il trasferimento e il trattamento, al fine di realizzare vantaggi economici. Le pronunce della Corte di Giustizia dell'UE *Schrems I* e *Schrems II* hanno mostrato come il settore dei dati personali si interfacci fortemente non solo con l'ambito economico ma anche con questioni di sicurezza nazionale degli Stati terzi importatori dei dati. Al fine di garantire la sicurezza nazionale, le autorità pubbliche dei Paesi esteri che mirano a importare dati di cittadini europei auspicano una deroga della normativa in materia di accesso ai dati personali. L'acceso ai dati è essenziale sotto il profilo della prevenzione del crimine per numerosi aspetti, tra i quali la prevenzione di delitti di stampo terroristico (e, in particolare, per l'individuazione dei membri delle associazioni a delinquere). Il diffondersi degli attacchi terroristici nei decenni passati aveva portato gli Stati Uniti ad adottare una normativa che consentisse l'accesso ai dati personali degli individui, da parte delle autorità governative, con estrema facilità con l'obiettivo di individuare preventivamente gli attentatori e il luogo dell'attentato. Inoltre, negli ultimi due anni, con la diffusione del virus Covid-19, la necessità di accedere ai dati sanitari degli individui ha assunto nuova rilevanza sotto il profilo della salute pubblica, al fine di arginare il più possibile la crescita della pandemia[7]. A situazioni eccezionali è derivata una risposta altrettanto eccezionale degli Stati, risposta che ha inevitabilmente portato all'agevolazione dell'accesso ai dati personali da parte delle autorità pubbliche a discapito dei diritti degli individui in materia.

Il compito dell'Unione europea appare allora ancora più gravoso in quanto, a fronte del regime di garanzie predisposto in materia di dati dall'Unione, l'esportazione degli stessi verso Stati terzi mediante gli strumenti previsti dal Regolamento (UE) n. 679/2016[8], spesso mossa da esigenze commerciali, può avvenire unicamente alla condizione che detti Stati rispettino in principi posti dall'Unione nel ricevere e trattare i dati personali. Sorge pertanto spontaneo domandarsi se il quadro normativo predisposto dall'Unione per operare il trattamento e il trasferimento di dati personali possa efficacemente garantire i

[6] Art. 16 Trattato sul Funzionamento dell'Unione europea del 26 ottobre 2012 (GU C 326/47).
[7] L. BRADFORD, M. ABOY, K. LIDDELL, *Standard contractual clauses for cross-border transfers of health data after Schrems II*, in *Journal of Law and the Biosciences*, n. 1, 2021, p. 4.
[8] Regolamento del Parlamento europeo e del Consiglio dell'Unione europea n. 2016/679 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) (GU L 119/1).

diritti degli individui senza cedere a deroghe al fine di concludere accordi commerciali con Stati che non presentano un sistema analogo di garanzie.

In particolare, il Regolamento (UE) n. 679/2016 disciplina le condizioni di trasferimento transfrontaliero[9] dei dati personali[10] dei soggetti interessati[11] oltre i confini dell'Unione europea nel

caso in cui questo non risulti direttamente applicabile agli importatori di dati stabiliti in Stati terzi ai sensi dell'art. 3 dello stesso (norma che disciplina l'ambito di applicazione territoriale del Regolamento). L'art. 44 del Regolamento Generale per la Protezione dei Dati (RGPD) dispone che qualsiasi trasferimento transfrontaliero possa avere luogo unicamente nel caso in cui i soggetti che lo operano rispettino le condizioni di cui al Capo V dello stesso. Quest'ultimo prevede che il trasferimento di dati verso Paesi terzi sia legittimo quando ricorrono, alternativamente, due ipotesi. La prima riguarda l'adozione, da parte della Commissione, ai sensi dell'art. 45 RGPD, di una decisione di adeguatezza del sistema giuridico di uno Stato terzo nel caso in cui questa, a seguito di una valutazione approfondita, ritenga che esso disponga di un livello di protezione dei dati sostanzialmente equivalente a quello dell'Unione. L'adozione della decisione consente di liberalizzare il flusso di dati verso tali Paesi, equiparando, dal punto di vista del trasferimento dei dati, il loro territorio a quello dell'Unione. La seconda, che trova applicazione in via sussidiaria rispetto alla prima, riguarda le garanzie adeguate fornite dall'importatore di dati stabilito al di fuori dei confini dell'Unione europea. Le garanzie possono essere costituite da strumenti di varia natura, elencati al secondo e terzo paragrafo dell'art. 46 RGDP e, tra questi, vi sono le clausole contrattuali standard (CCS). Queste ultime rappresentano, nella prassi, lo strumento giuridico più utilizzato dalle imprese per trasferire dati qualora non vi sia la decisione di adeguatezza[12]. Le clausole contrattuali tipo vengono adottate dalla Commissione o da un'autorità garante per la protezione dei dati per poi essere

[9] Pur non essendo stata fornita una definizione di «trasferimento transfrontaliero dei dati personali» né dal Regolamento (UE) n. 2016/679 né dalla Corte di Giustizia dell'Unione europea, questa si può ricavare dalle recenti Linee guida del Comitato Europeo per la Protezione dei Dati del 2021. Con trasferimento di dati personali si intende l'operazione effettuata dall'esportazione di dati personali, che ha sede in uno Stato membro, verso un importatore di dati, che ha sede in uno Stato terzo. In base a quanto affermato dalla CGUE è possibile qualificare il trasferimento transfrontaliero di dati quale trattamento degli stessi («operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione»). Conseguentemente, le norme del RGPD in materia di trattamento di dati si applicano anche ai trasferimenti degli stessi.

[10] L'art. 4 del Regolamento (UE) n. 2016/679 definisce dato personale come: «qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale».

[11] Con «soggetto interessato» si intende l'individuo i cui dati personali sono oggetto di trattamento o trasferimento.

[12] N. CORY, E. DICK, D. CASTRO, *The Role and Value of Standard Contractual Clauses in EU-US Digital Trade*, in *Information Technology & Innovation Foundation*, 2020.

approvate dalla Commissione stessa mediante il meccanismo disposto dall'art. 93, para. 2, e consistono in un testo normativo sottoscritto congiuntamente dall'importatore di dati localizzato in uno Stato terzo e dall'esportatore localizzato in uno Stato membro. Il testo è giuridicamente vincolante per entrambe le parti, che sono tenute al suo rispetto, con l'obiettivo di garantire una protezione adeguata dei dati personali oggetto del trasferimento. Il contenuto delle norme è predefinito dalla Commissione europea e, pertanto, non possono essere modificate a seconda delle esigenze commerciali e della finalità del trattamento. Lo scopo che le clausole contrattuali standard perseguono è quello di salvaguardare i diritti fondamentali spettanti all'interessato; scopo che risulta essere esterno alle finalità che spingono importatore ed esportatore di dati a concludere un contratto.

La *ratio* di entrambe le categorie di basi giuridiche è quella di garantire che i dati dei soggetti interessati trasferiti oltre i confini degli Stati membri rimangano assoggettati ai medesimi standard di protezione previsti dalla disciplina europea. In altri termini, si vuole assicurare che i soggetti interessati, i cui dati sono oggetto di trasferimento transfrontaliero, possano godere delle tutele previste dalla normativa europea indipendentemente dal fatto che i dati vengano trattati all'interno o all'esterno del territorio dell'UE.

L'articolo si propone di fornire un quadro dell'evoluzione delle basi giuridiche maggiormente impiegate nelle prassi al fine di operare il trasferimento dei dati oltre i confini dell'Unione europea con specifico riferimento all'accesso ai dati personali da parte delle autorità pubbliche degli Stati terzi. Nell'effettuare l'analisi, imprescindibile sarà il riferimento alle sentenze *Schrems I* e *Schrems II* della Corte di Giustizia dell'Unione europea, che hanno orientato fortemente lo sviluppo della decisione di adeguatezza e delle clausole contrattuali standard. Detto studio consentirà di effettuare una disamina della nuova decisione della Commissione inerente alle CCS con riguardo alle misure da questa adottate al fine di far fronte alle criticità sollevate dalla Corte in merito all'accesso ai dati da parte delle autorità nazionali degli Stati ove i dati vengono importati.

2. La decisione di adeguatezza e l'accesso ai dati personali da parte delle autorità governative degli Stati terzi nelle pronunce *Schrems I* e *Schrems II*

L'art. 46 del Regolamento (UE) n. 679/2016 definisce la decisione di adeguatezza come la «formale attestazione da parte della Commissione in merito all'adeguatezza della protezione dei dati personali nel Paese terzo o organizzazione internazionale». I parametri che la Commissione prende in considerazione al fine di valutare se il livello di tutela dei dati personali di uno Stato terzo sia equivalente a quello

dell'Unione sono previsti dall'art. 45, para. 2, del Regolamento[13]. I molteplici aspetti dei quali la Commissione deve tenere conto rispecchiano i principi e le norme sulle quali uno Stato, in grado di garantire una protezione adeguata dei suoi cittadini, si fonda. Tuttavia, non si può negare come il vaglio della Commissione dipenda altrettanto (e in buona misura) da valutazioni politiche e, in particolare, legate alla convenienza di *partnership* commerciali con Stati esteri. La dottrina è concorde nell'affermare che, durante gli ultimi decenni, si è assistito alla politicizzazione degli accordi commerciali dell'Unione. Il fenomeno è stato definito come «*increase in polarization of opinions, interests or values and the extent to which they are publicly advanced to-wards the process of policy formulation*»[14]. La politicizzazione delle decisioni commerciali europee ha notevoli conseguenze non solo per la politica commerciale estera. Invero, tale fenomeno si riflette anche sull'ambito del trasferimento transfrontaliero dei dati, portando l'Unione ad agevolare l'esportazione di dati personali verso determinati Paesi terzi nei confronti dei quali è stato adottato un accordo commerciale.

La valutazione sull'adeguatezza, che si traduce in una valutazione nel merito, seppur sulla base di alcuni precisi parametri, è stata frutto di un'evoluzione nel lungo periodo, caratterizzata da pronunce della CGUE che hanno profondamente influenzato la definizione dei parametri in un'ottica pratica. La Corte di Giustizia dell'Unione europea, mediante le storiche sentenze *Schrems I* e *Schrems II*, ha fissato principi fondamentali in materia di trasferimento transfrontaliero di dati, determinando un cambiamento significativo nell'impiego della decisione di adeguatezza. Le pronunce della Corte di Giustizia hanno portato alla luce le fragilità dell'istituto dell'art. 45 del Regolamento (UE) 2016/679 nel garantire la protezione dei dati personali nei trasferimenti transfrontalieri, rendendo necessarie modifiche sistemiche in materia. In particolare, tale fragilità è emersa con riguardo all'accesso indiscriminato ai dati personali da parte delle autorità pubbliche statunitensi. Questo ha determinato una grave violazione delle garanzie europee; violazione perpetrata proprio tramite lo strumento a cui spetta, al contrario, il compito di tutelare detti diritti.

[13] Tra questi vi sono l'assetto normativo del Paese importatore di dati, che deve garantire il rispetto dei diritti umani fondamentali, la previsione e l'attuazione di garanzie adeguate di protezione dei dati, la disciplina dei trasferimenti transfrontalieri, la giurisprudenza e i diritti effettivi e azionabili degli interessati, l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti che possa assicurare il rispetto delle norme in materia di protezione dei dati e, infine, l'agenda di impegni internazionali che l'importatore si assume in relazione alla protezione dei dati.

[14] P. DE WILDE, *No polity for old politics? A frame-work for analyzing the politicization of Europeanintegration*, in *Journal of European Integration*, n. 5, 2011, pp. 559–575.

2.1. I parametri fissati dalla sentenza *Schrems I* per l'accesso ai dati da parte delle autorità governative dello Stato destinatario della decisione di adeguatezza

La sentenza *Schrems I*[15] ha avuto, quale effetto principale, l'invalidazione del sistema *Safe Harbour*, insieme di principi recepiti nella decisione di adeguatezza della Commissione europea n. 2000/520/CE[16], avente come destinatario gli Stati Uniti. Tali principi rappresentavano il frutto di una complessa trattativa intercorsa tra il governo statunitense e le istituzioni europee dopo l'entrata in vigore della Direttiva n. 95/46/CE[17]. Lo scopo dei negoziati, durati più di due anni[18], era quello di «*fill in what the EU viewed as inadequacies, or gaps, in the US data privacy protection*»[19]. Essendo costituito da atti unilaterali adottati sia dalla Commissione europea che dal governo statunitense, la natura giuridica del *Safe Harbuor* non era quella di accordo di diritto internazionale, nonostante fosse frutto di un negoziato tra UE e USA volto a regolare il flusso transnazionale di dati tra soggetti privati[20]. Pertanto, il *Safe Harbour* era basato sulla volontarietà delle aziende statunitensi di aderire al sistema di principi e di tutele da questo configurato in ambito di protezione dei dati personali degli interessati, ovvero i cittadini europei, i cui dati venivano esportati verso gli USA[21]. Volontarietà che, tuttavia, era circoscritta alle sole organizzazioni operanti negli Stati Uniti nell'ambito dei settori sottoposti al controllo «*of a government body in the United States listed in Annex VII of the Decision which is empowered to investigate Complaints and to obtain relief against unfair and deceptive practices*»[22]. Le autorità previste dall'Allegato VII erano la *Federal Trade Commission* (FTC) e il *Department of Transportation* e, pertanto, non erano sottoposte alla disciplina delineata nella decisione di adeguatezza tutte le operazioni di trasferimento dei dati condotte da organizzazioni aventi carattere o funzione pubblica[23].

---

[15] CGUE, causa C-362/14, *Maximillian Schrems c. Data Protection Commissioner*, con l'intervento di: *Digital Rights Ireland Ltd.*, sentenza del 6 ottobre 2015.

[16] Decisione della Commissione n. 2000/520/CE del 26 luglio 2000 a norma della Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del Commercio degli Stati Uniti (GU L 215).

[17] Direttiva del Parlamento europeo e del Consiglio dell'Unione europea n. 95/46/CE del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (GU L 281/31).

[18] Durante questo periodo di tempo l'Unione europea aveva deciso di sospendere il suo diritto di interrompere l'esportazione dei dati verso gli Stati Uniti in quanto erano in corso delle trattative mediante una serie di incontri ufficiali e scambi di corrispondenza. La durata dei negoziati era dovuta alla necessità che il sistema statunitense introducesse garanzie analoghe a quelle previste dalla disciplina europea per la protezione dei dati, al fine di poter adottare la decisione di adeguatezza.

[19] W. J. LONG, M. P. QUEK, *Personal Data Privacy Protection in an Age of Globalization: The US-EU Safe Harbor Compromise*, in *Journal of European Public Policy*, n. 3, 2002, p. 335.

[20] S. SALUZZO, *The EU as a Global Standard Setting Actor: The Case of Data Transfers to Third Countries*, in E. CARPANELLI, N. LAZZERINI (a cura di), *Use and Misuse of New Technologies. Contemporary Challenges in International and European Law*, Springer Nature Switzerland, Cham, 2019, p. 129.

[21] S. SICA, V. D'ANTONIO, *I Safe Harbour Principles: genesi, contenuti, criticità*, in *Diritto dell'informazione e dell'informatica*, n. 4-5, 2015, p. 808.

[22] Art. 2, lett. a) e b), Decisione n. 2000/520/CE, *cit.*

[23] *Ibid.*, allegato VII.

Per comprendere il sistema statunitense di regolamentazione dei dati personali occorre fare un passo indietro. Alla fine degli anni '90 la FTC, da un lato, era favorevole alla autoregolamentazione del settore mediante l'adozione di codici di comportamento da parte delle aziende che trattavano i dati, nonché di *privacy policy*, mentre, dall'altro, era consapevole che l'autoregolamentazione non era sufficiente a garantire la protezione dei dati dei consumatori sul web. Pertanto, nel 2000, la *Federal Trade Commission* sottoscrisse un rapporto che invitava a regolamentare il trattamento dei dati personali online mediante la legge[24]. Gli attentati terroristici dell'11 settembre 2001 determinarono però un brusco cambiamento di rotta, facendo sì che il focus si spostasse sulla sicurezza, tralasciando la *privacy* degli individui[25]. Il Congresso statunitense approvò il *Patriot Act*, ideò il *Terrorist Screening Program,* adottando, inoltre, una serie di ulteriori misure per agevolare e ampliare la raccolta di dati personali al fine di prevenire il terrorismo. Nel 2002 la *Advanced Research and Developement Activity* del Pentagono ricevette un finanziamento di 64 milioni di dollari per lo sviluppo di un programma di ricerca sulle nuove attività di intelligence ricavate dai *big data*. Le autorità di pubblica sicurezza statunitensi erano strettamente dipendenti dalle aziende che già conducevano operazioni sui dati personali degli individui a fini commerciali[26]. Ciò ha fatto sì che il vuoto legislativo consentisse alle aziende private di giovare sostanzialmente alla stessa emancipazione dalla legge (per motivi appunto di pubblica sicurezza) delle autorità governative.

In seguito allo scandalo *Datagate*, il Parlamento europeo aveva approvato una Risoluzione che esprimeva il timore per le operazioni condotte mediante il programma PRISM e altri programmi di sorveglianza, chiedendo agli Stati Uniti di fornire senza ritardo ulteriori informazioni sulle azioni di spionaggio condotte ai danni dell'UE[27]. Il Parlamento aveva inoltre incaricato la Commissione parlamentare per le libertà civili di svolgere un'indagine in merito. Nel 2013, mediante una successiva Risoluzione, il Parlamento europeo, quale conseguenza delle presunte intercettazioni condotte dalla *National Security Agency* (NSA) sulle informazioni bancarie di alcuni cittadini europei collegati alla società belga SWIFT, aveva sollecitato la sospensione dell'accordo con gli Stati Uniti avente a oggetto il programma *Terrorist Finance Tracking*[28].

A fronte della forte ingerenza operata dai servizi di intelligence statunitensi a discapito del diritto alla riservatezza dei cittadini europei, la Corte di Giustizia dell'UE è intervenuta in maniera incisiva sul *Safe*

[24] S. ZUBOFF, *Il Capitalismo della Sorveglianza. Il Futuro dell'umanità nell'era dei Nuovi Poteri*, Luiss University Press, Roma, 2019, p. 124.
[25] S. LEVY, *How Google Thinks, Works, and Shapes our Lives*, Simon & Schuster, New York, 2011, p. 13.
[26] D. EDWARDS, *I'm Feeling Lucky: The Confessions of Google Employee Number 59*, Mariner Books, Boston, 2012, pp. 340-345.
[27] Risoluzione legislativa del Parlamento europeo del 4 luglio 2013 sulla proposta di direttiva del Parlamento europeo e del Consiglio relativa agli attacchi contro i sistemi di informazione, e che abroga la decisione quadro 2005/222/GAI del Consiglio (COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)).
[28] Risoluzione del Parlamento europeo del 23 ottobre 2013 sulla sospensione dell'accordo TFTP a seguito della sorveglianza dell'Agenzia per la sicurezza nazionale statunitense (2013/2831(RSP)).

Harbour al fine di evitare il perpetrarsi di un abbassamento delle garanzie europee guidato da opportunità economiche e commerciali con le imprese statunitensi[29]. Il 6 ottobre 2015 la Corte di Giustizia dell'Unione europea ha quindi adottato la sentenza definitiva per il caso *Schrems c. Data Protection Commissioner*, dichiarando l'invalidità del *Safe Harbour* e annullando la decisione n. 2000/520/CE[30]. Ciò ha avuto, come immediata conseguenza, l'interruzione dei trasferimenti di dati tra Unione Europea e Stati Uniti, che fino ad allora avvenivano sulla sola base della decisione della Commissione, costringendo gli importatori di dati statunitensi a rispettare le altre condizioni previste dalla Direttiva n. 95/46/CE per operare il trasferimento[31]. A questa si può attribuire, inoltre, il merito di aver attirato l'attenzione dei cittadini, sia europei che statunitensi, sul tema della sorveglianza di massa e sulla necessità di bilanciare la sicurezza nazionale con il rispetto del diritto alla *privacy* quale diritto fondamentale[32].

Nonostante la pronuncia abbia trattato diversi aspetti inerenti alla normativa sulla protezione dei dati, occorre in questa sede soffermarsi specificatamente sui principi disposti dalla stessa in tema di accesso ai dati personali da parte delle autorità pubbliche degli Stati terzi importatori.

---

[29] Opportunità che, in una certa misura, anche oggi continuando a spingere l'Europa a concedere alcuni significativi benefici alle aziende nordamericane, «nella consapevolezza che il rapporto di forza UE-USA ha natura diversa di quello che esiste fra l'Unione e altri Paesi terzi» (A. MANTELERO, *L'ECJ invalida l'accordo per il trasferimento dei dati personali fra EU ed USA. Quali scenari per cittadini ed imprese?*, in *Contratto e Impresa. Europa*, n. 2, 2015, p. 722).

[30] Il caso originava dal cittadino austriaco e utente *Facebook* Maximillian Schrems, il quale, mediante una serie di ricorsi, è stato in grado di sfidare il trasferimento di dati operato da *Facebook* verso gli Stati Uniti in base al *Safe Harbour*. Schrems, a partire dal 2011, ha condotto una serie di ricorsi nei confronti della filiale irlandese di *Facebook Inc.*, sede europea principale della multinazionale americana, lamentando la violazione di numerosi principi in tema di protezione dei dati personali, che hanno condotto alla modifica di alcune *privacy policy* dell'azienda. In particolare, affermava che tutti gli utenti europei del *social network* erano tenuti a siglare un contratto con la filiale Europea con sede in Irlanda e che, di conseguenza, le informazioni raccolte venivano trasferite verso i server nordamericani. Nel 2013, Schrems si rivolgeva quindi all'autorità di controllo irlandese chiedendo la sospensione del trasferimento dei dati dall'Irlanda agli Stati Uniti, sostenendo che negli USA non fosse garantito un adeguato livello di protezione dei dati personali. Egli affermava che, in base alle accuse mosse da Edward Snowden, la *National Security Agency* (NSA) statunitense, mediante il programma di intercettazioni PRISM, avrebbe avuto il diritto di accedere a una serie di dati personali contenuti in archivi virtuali, attuando un'attività di sorveglianza di massa anche sui dati dei cittadini europei. Edward Snowden, figura di rilievo nello scandalo *Datagate*, è un ex dipendente informatico della *Central Intelligence Agency* (CIA) che ha denunciato all'opinione pubblica l'attività di sorveglianza su larga scalda perpetrata dalla NSA. Il Commissario irlandese per la Protezione dei Dati rigettava le questioni sollevate da Schrems nel ricorso, affermando di non avere l'autorità per indagare sull'adeguatezza del sistema nordamericano di tutela dei dati, in quanto questo era già stato ritenuto adeguato dalla Commissione. Egli proponeva dunque appello innanzi all'*Hight Court of Irland*, la quale ha disposto che l'accesso generalizzato ai dati da parte della NSA si poneva in netto contrasto con i principi fondamentali affermati sia nella Costituzione irlandese che dagli artt. 7, 8 e 52 della Carta dei Diritti Fondamentali dell'UE. La Corte, ritenendo fondati i dubbi sollevati circa l'adeguatezza del sistema statunitense, rivolgeva alla CGUE una questione pregiudiziale concernente la competenza delle autorità di controllo a conoscere e decidere su ricorsi proposti dagli interessati nel caso in cui vi fosse una decisione di adeguatezza in precedenza adottata dalla Commissione.

[31] Comunicazione della Commissione europea al Parlamento europeo e al Consiglio dell'Unione Europea del 6 novembre 2015 relativa al trasferimento di dati personali dall'UE agli Stati Uniti d'America in applicazione della direttiva 95/46/CE a seguito della sentenza della Corte di giustizia nella causa C-362/14, (*Schrems*) (GU COM/566).

[32] M. S. VIDOVIĆ, *Schrems v. Data Protection Commissioner (case c-362-14): Empowering National Data Protection Authorities*, in *Croatian Yearbook of European Law and Policy*, n. 1, 2015, p. 258.

La Corte ha effettuato tre constatazioni preliminari. Innanzitutto, ha rilevato come i principi del *Safe Harbour* fossero applicabili unicamente agli importatori di dati statunitensi che autocertificavano il rispetto di tali principi, senza però esigere il rispetto degli stessi da parte delle autorità pubbliche[33]. In secondo luogo, ha messo in luce come la decisione di adeguatezza non avesse tenuto adeguatamente in considerazione l'art. 25, para. 6, della Direttiva, il quale richiedeva la sussistenza di un livello di protezione dei dati personali adeguato del Paese destinatario in considerazione della legislazione nazionale dello Stato importatore e dei suoi impegni internazionali[34]. La normativa statunitense, che consentiva l'accesso indiscriminato da parte delle autorità di intelligence ai dati personali dei soggetti interessati, non risultava in alcun modo rispettosa della norma[35]. In terzo luogo, la Corte ha rilevato come l'applicabilità dei principi previsti dalla decisione poteva essere limitata unicamente «se ed in quanto necessario per soddisfare esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia [degli Stati Uniti]»[36]. Di conseguenza, la decisione stabiliva il primato delle esigenze di sicurezza nazionale, nonché di interesse pubblico e di amministrazione della giustizia, sui principi previsti dalla decisione di adeguatezza. In forza di questo primato «le organizzazioni americane autocertificate che ricevono dati personali dall'Unione sono tenute a disapplicare senza limiti tali principi allorché questi ultimi interferiscono con tali esigenze e risultano dunque incompatibili con le medesime»[37].

Alla luce di queste considerazioni, la Corte ha rilevato come le ingerenze nei diritti fondamentali degli individui, i cui dati venivano importati negli Stati Uniti, operate da parte delle autorità governative per esigenze di sicurezza nazionale, non rivestivano carattere eccezionale e non possedevano alcuna limitazione da parte della legge, senza che agli interessati spettasse alcun mezzo di ricorso giurisdizionale. Ciò costituiva una gravissima violazione dei diritti fondamentali dell'individuo previsti dagli artt. 7, 8, 47 e 52 della Carta dei Diritti Fondamentali dell'UE.

Ai sensi dell'art. 52 della Carta, eventuali limitazioni all'esercizio dei diritti e delle libertà fondamentali riconosciute dalla stessa devono essere previste dalla legge e rispettare, in ogni caso, il nucleo essenziale dei diritti e delle libertà. Inoltre, le eventuali limitazioni devono, nel rispetto del principio di proporzionalità, essere adottate unicamente quando siano necessarie e rispondano a esigenze di interesse generale riconosciute dall'Unione o di protezione dei diritti e delle libertà altrui[38]. Pertanto, qualsiasi

[33] CGUE, *Maximillian Schrems c. Data Protection Commissioner*, *cit.,* punto 82.
[34] *Ibid.*, punto 83.
[35] Ciò a maggior ragione se si considera che molto spesso i dati trattati dalle autorità derivavano direttamente da aziende che importavano tali dati dall'Unione e che autocertificavano il rispetto dei principi del *Safe Harbour*.
[36] CGUE, *Maximillian Schrems c. Data Protection Commissioner*, *cit.*, punto 84.
[37] *Ibid.*, punto 86.
[38] R. CISOTTA, in *Brevi note sulla giurisprudenza dell'art. 52, par. 1 della Carta dei Diritti Fondamentali dell'UE in materia di limitazioni ai diritti fondamentali* (2021), rileva come i criteri per l'ammissibilità delle limitazioni ai diritti fondamentali sono previsti da due frasi distinte dell'art. 52. Nella prima frase si pone una riserva di legge per le limitazioni all'esercizio dei diritti fondamentali e si stabilisce che esse devono rispettare il contenuto essenziale di detti diritti e libertà. Sul punto, la

normativa dell'Unione che comporti un'ingerenza nei diritti fondamentali garantiti dagli artt. 7 e 8 della Carta, inerenti al rispetto della vita privata e famigliare e alla protezione dei dati personali, deve necessariamente disporre «regole chiare e precise che disciplinino la portata e l'applicazione della misura *de qua*»[39], prevedendo garanzie sufficienti che permettano ai soggetti interessati di proteggere i loro dati contro il rischio di abusi ed eventuali accessi e usi illeciti. Una normativa che autorizzi in maniera generale la conservazione di tutti i dati personali degli individui trasferiti dall'Unione verso gli Stati Uniti senza alcun criterio oggettivo che permetta di delimitare l'accesso da parte delle autorità pubbliche, nonché il loro impiego a fini precisi, rigorosamente ristretti e idonei a giustificare l'ingerenza che l'accesso e l'utilizzazione ai dati comportano, non può considerarsi una restrizione alla tutela dei dati personali operante nei limiti dello stretto necessario[40], risultando in una grave violazione degli artt. 7 e 8 della Carta di Nizza[41]. Inoltre, l'assenza di una normativa che preveda la possibilità del soggetto interessato di avvalersi di rimedi giuridici al fine di accedere ai dati personali che lo riguardano, ovvero di ottenerne la rettifica o la soppressione, non è rispettosa del diritto fondamentale a una tutela giurisdizionale effettiva così come disposto dall'art. 47 della Carta.

Diventando i diritti fondamentali della Carta parametri di valutazione dell'adeguatezza del regime di protezione dei dati personali in uno Stato terzo, la Corte ha pertanto dichiarato l'invalidità della decisione n. 2000/520/CE[42], ritenendo che il regime di tutela dei dati personali predisposto dagli Stati Uniti non era sostanzialmente equivalente a quello dell'Unione Europea.

2.2. L'evoluzione dei parametri in *Schrems II*

Dopo l'invalidazione della decisione di adeguatezza n. 2000/520/CE, le clausole contrattuali tipo erano diventate, di fatto, lo strumento più impiegato al fine di trasferire i dati agli Stati Uniti. Tuttavia, la Commissione europea, anche grazie alle pressioni delle imprese europee e statunitensi, aveva incrementato le trattative intraprese con gli USA, già in atto a partire dal 2013, per apportare migliorie al

CGUE ha osservato che il contenuto essenziale del diritto è identificabile nella sostanza stessa di questo (CGUE, causa C-292/97, *Kjell Karlsson e a.*, sentenza del 13 aprile 2000, punto 45). Nella seconda frase si impone il rispetto del principio di proporzionalità e si prescrive che le limitazioni in questione possono essere ammesse «solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui». Secondo costante giurisprudenza della Corte di Giustizia, per quanto concerne il controllo giurisdizionale del rispetto delle condizioni di cui alla norma in esame, «allorché si tratta di ingerenze in diritti fondamentali, la portata del potere discrezionale del legislatore dell'Unione può risultare limitata in funzione di un certo numero di elementi, tra i quali figurano, in particolare, il settore interessato, la natura del diritto di cui trattasi garantito dalla Carta, la natura e la gravità dell'ingerenza nonché la finalità di quest'ultima» (CGUE, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a.* e *Kärntner Landesregierung e a.*, sentenza dell'8 aprile 2014, punto 47).

[39] CGUE, *Maximillian Schrems c. Data Protection Commissioner*, *cit.*, punto 91.

[40] *Ibid.*, punto 93.

[41] *Ibid.*, punto 94.

[42] *Ibid.*, punti 96-98.

Safe Harbour, arrivando all'adozione di un nuovo accordo: il *Privacy Shield*. Il 12 luglio 2016 la Commissione cristallizzava, anche questa volta senza non poche difficoltà[43], il frutto delle trattative tra Unione e Stati Uniti nella decisione (UE) n. 2016/1250[44]. Fin dalla sua entrata in vigore, il primo agosto del 2016, ci si domandava se il *Privacy Shield* costituisse un meccanismo di protezione dei dati migliore del suo predecessore e se avesse effettivamente integrato i parametri previsti nella sentenza *Schrems I*[45].

Nonostante i sette principi del *Privacy Shield* fossero sostanzialmente analoghi a quelli del *Safe Harbour*, alcune misure ulteriori e garanzie erano state introdotte al fine di allinearsi con quanto disposto dalla Corte di Giustizia nella sentenza *Schrems I*[46]. Rilevanti erano invece le limitazioni all'accesso ai dati da parte delle autorità pubbliche introdotte dal governo statunitense, contenute in una serie di lettere provenienti dal governo degli Stati Uniti e facenti parte della nuova decisione della Commissione. In particolare, la lettera del Segretario di Stato prevedeva l'impegno a instituire un mediatore per le inchieste relative all'accesso ai dati da parte dei servizi di intelligence degli USA, detto *Ombudsperson*[47]. In un'altra lettera proveniente dal Ministero della Giustizia si configuravano una serie di salvaguardie e limitazioni all'accesso ai dati da parte delle autorità pubbliche ai fini dell'applicazione della legge nazionale per motivi di interesse pubblico[48]. Infine, la lettera dell'*Office of the Director of National Intelligence* predisponeva una ulteriore serie di restrizioni applicabili alle autorità di sicurezza nazionali, prevedendo che la *President Policy Directive* (PPD-28) avrebbe garantito la tutela della *privacy* e dei dati personali indipendentemente dalla nazionalità degli interessati a cui i dati erano ascrivibili[49].

Sulla base delle dichiarazioni formali del governo statunitense la Commissione aveva ritenuto che, conformemente a quanto affermato dalla Corte di Giustizia nella sentenza *Schrems I*, il regime di protezione dei dati personali degli Stati Uniti, grazie all'introduzione delle limitazioni all'ingerenza delle pubbliche autorità nei diritti fondamentali degli interessati europei a fini di sicurezza nazionale, nonché alla previsione del diritto degli interessati di agire giudizialmente, fosse sostanzialmente equivalente a

[43] Il Gruppo di Lavoro Articolo 29, nel parere n. 1/2016, integrando quanto osservato dalla Corte di Giustizia, ha rilevato come il livello di protezione del *Privacy Shield* non poteva essere ritenuto adeguato alla luce di una serie di motivi quali, ad esempio, la mancanza della possibilità, per i cittadini europei interessati dal trasferimento dei dati, di esercitare mezzi di ricorso giurisdizionale effettivi e la mancanza del rispetto del requisito di stretta necessarietà e proporzionalità nella raccolta dei dati.

[44] Decisione di esecuzione della Commissione (UE) n. 2016/1250 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 (GU L 207/2016).

[45] F. TERPAN, *EU-US Data Transfer from Safe Harbour to Privacy Shield: Back to Square One?*, in *European papers*, n. 3, 2018, p. 1050.

[46] Quale, ad esempio, il principio di «*resorurce, enforcement and liability*».

[47] Allegato III, Decisione (UE) n. 2016/150, *cit.*

[48] *Ibid.*, allegato VII.

[49] *Ibid.*, allegato VI.

quello dell'Unione[50]. Tuttavia, la Corte è arrivata a una considerazione opposta in quanto la decisione di adeguatezza disponeva che l'adesione ai principi ivi previsti poteva comunque essere limitata nella misura necessaria per soddisfare la sicurezza nazionale, l'interesse pubblico o esigenze di applicazione della legge domestica[51]. Questa previsione appariva pertanto vanificare i tentativi di limitazione dell'accesso ai dati personali dei cittadini europei da parte delle autorità di intelligence statunitensi.

La Corte di Giustizia, nel valutare la decisione di adeguatezza, ha fatto riferimento all'art. 52 della Carta di Nizza, sottolineando come il requisito di proporzionalità implicasse necessariamente che le norme che prevedevano tale ingerenza avrebbero dovuto rispettare due requisiti minimi. In primo luogo, essere chiare e precise nel disciplinare la portata e la modalità dell'interferenza, indicando le circostanze e le condizioni a cui questa può avvenire. In secondo luogo, prevedere delle garanzie minime per tutelare i diritti dei soggetti interessati, i cui dati sono oggetto di ingerenza, a fronte di possibili abusi.

Alla luce di detti requisiti, la CGUE ha rilevato come alle agenzie di intelligence statunitensi spettasse, nonostante le modifiche introdotte in materia, un potere estremamente ampio di effettuare sorveglianza di massa praticamente illimitata sui dati dei cittadini europei ai fini di sicurezza nazionale[52]. La Corte, nell'esaminare il regime degli Stati Uniti concernete il livello di protezione dei dati, ha preso in considerazione tre atti differenti: la *Section 702 of FISA*, la PPD-28 e l'*Executive Order 12333*[53]. Con riguardo al primo atto normativo, che consentiva l'adozione di programmi di sorveglianza di massa dei dati personali e non singole specifiche misure, ha osservato come non fosse previsto alcun tipo di limitazione nell'attuazione del programma da parte delle autorità di intelligence o la possibilità, per i cittadini europei i cui dati facevano parte dell'attività di controllo, di ricorrere in via giurisdizionale[54]. Inoltre, anche la PPD-28, il cui scopo era quello stabilire le condizioni sulla base delle quali potevano essere realizzate tali operazioni, non prevedeva alcun mezzo di ricorso giurisdizionale, per i soggetti interessati, esercitabili nei confronti delle autorità statunitensi[55]. Lo stesso valeva per l'ultimo atto normativo menzionato, l'*Executive Order 12333*, volto ad autorizzare programmi di sorveglianza di massa che garantivano l'accesso ad ampie categorie di dati, tra le quali quelli provenienti dai cittadini europei, senza che, anche in questo caso, fosse stabilito in maniera chiara né l'operato delle autorità di intelligence né la possibilità di esercitare rimedi giurisdizionali.

---

[50] M. H. MURPHY, *Assessing the Implications of Schrems II for EU-US Data Flow*, in *International and Comparative Law Quarterly,* n. 1, 2022, p. 253.
[51] *Ibid.*, punti 163-164.
[52] *Ibid.*, punto 180.
[53] *Section 702*, *Foreign Intelligence Surveillance Act of 1978* (122 Stat. 2436); *Executive Order 12333*; *President of the United States of America, «Presidential Policy Directive 28»* (PPD-28) del 17 gennaio 2014.
[54] M. NINO, *La sentenza Schrems II della Corte di giustizia UE*, *cit.*, p. 749.
[55] CGUE, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems*, *cit.*, punto 181.

In forza di dette considerazioni, la Corte ha ritenuto che nessuno di tali atti fosse in grado di rispettare il principio di proporzionalità, «cosicché non si può considerare che i programmi di sorveglianza basati su tali disposizioni siano limitati allo stretto necessario»[56]. La mancata limitazione dell'accesso delle autorità statunitensi alle banche dati contenenti informazioni provenienti da Stati membri ha determinato la non conformità dell'ordinamento nordamericano ai parametri di tutela previsti dall'Unione. Pertanto, la CGUE ha dichiarato l'invalidità, con effetto immediato, del *Privacy Shield*, confermando la non correttezza della valutazione della Commissione nell'adottare la decisione di adeguatezza nei confronti degli Stati Uniti, determinando l'illegittimità *ex nunc* del trasferimento transfrontaliero di dati verso gli USA attuati sulla base della decisione (UE) n. 2016/1250.

La pronuncia adottata dalla CGUE nel caso *Schrems II* assume particolare importanza su diversi paini, non solo per aver ridefinito la portata di numerosi principi in tema di trasferimento e trattamento dei dati ma anche per l'impatto prodotto sia a livello giuridico che commerciale[57]. La sentenza, da un lato, costituisce un *unicum* giurisprudenziale con il sentiero tracciato a partire dalla pronuncia *Schrems I* e, dall'altro, ne rappresenta una notevole evoluzione. La sentenza *Schrems II* rafforza l'orientamento giurisprudenziale che, da ormai un decennio, cercava di consolidare uno standard di tutela potenziata in tema di protezione dei dati personali[58], così come configurato anche nel Regolamento (UE) n. 2016/679. L'interpretazione della Corte ha elevato gli artt. 7, 8, 47 e 52 della Carta dei Diritti Fondamentali dell'UE a parametri sui quali calibrare le intrusioni delle autorità governative nei diritti degli individui, permettendo di effettuare una valutazione sulla validità della decisione di adeguatezza fondata sul rispetto di tali diritti.

3. Le clausole contrattuali standard e l'accesso ai dati personali da parte delle autorità governative degli Stati terzi nella pronuncia *Schrems II*

Le clausole contrattuali standard sono qualificate dal Regolamento (UE) n. 2016/679 quali basi giuridiche sussidiarie per operare il trasferimento extraeuropeo dei dati personali. L'art. 46 RGDP dispone che esse possono essere impiegate nel caso in cui non sia stata adottata una decisione di adeguatezza nei confronti dello Stato terzo o organizzazione internazionale destinataria dei dati[59]. Le clausole, così come gli altri

[56] *Ibid.*, punto 184.
[57] M. NINO, *La sentenza Schrems II della Corte di giustizia UE*, *cit.*, p. 750.
[58] CGUE, cause riunite C-203/15 e C-698/15, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Ireland, The Attorney General*, sentenza dell'8 aprile 2014; causa C-131/12, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 maggio 2014; cause riunite C-203/15 e C-698/15, *Tele2 Servige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson, Peter Brice, Geoffrey Lewis*, con l'intervento di: Open Rights Group, Privacy International, The Law Society of England and Wales, sentenza del 21 dicembre 2016.
[59] Art. 46, para. 1, Regolamento (UE) n. 2016/679, *cit.*

istituti previsti dalla norma in esame, rientrano nella categoria delle «garanzie adeguate» al fine di operare il trasferimento. I considerando 108 e 114 del Regolamento definiscono come adeguate quelle garanzie che siano in grado di «compensare la carenza di protezione dei dati di un Paese terzo […] a tutela dell'interessato»[60]. Si tratta di tutele che l'esportatore di dati ha l'onere di adottare al fine di garantire all'interessato che i diritti connessi al trattamento dei propri dati continuino a trovare applicazione anche al di fuori dell'Unione europea[61].

La Corte, nella pronuncia *Schrems II*, non solo ha dichiarato l'invalidità del *Privacy Shield* ma ha dedicato particolare attenzione alla legittimità dei trasferimenti dei dati verso tutti gli Stati terzi effettuati mediante l'utilizzo delle clausole contrattuali standard. Invero, l'invalidazione della decisione di adeguatezza n. 2000/520/CE ha determinato un notevole aumento dell'impiego delle clausole contrattuali tipo al fine di operare trasferimenti di dati verso gli Stati Uniti. Tutt'oggi, a fronte della sentenza *Schrems II*, che ha invalidato la successiva dichiarazione di adeguatezza nei confronti degli Stati Uniti, le CCS rivestono un ruolo di assoluto rilievo nel trasferimento transfrontaliero di dati personali.

Per comprendere la decisione della Corte in merito alle clausole contrattuali tipo occorre effettuare un breve riferimento alla vicenda che ha portato all'adozione della sentenza *Schrems II*. In seguito alla pronuncia *Schrems I*, l'autorità di controllo irlandese aveva avviato una serie di indagini nei confronti della filiale di *Facebook* in Irlanda, invitando Schrems a riformulare i motivi di ricorso da lui presentati alla luce dell'intervenuta pronuncia della Corte europea. Allo stesso tempo, la multinazionale era passata, così come la stragrande maggioranza delle altre imprese, a operare il trasferimento sulla base delle clausole contrattuali tipo. Nel riformulare i motivi di ricorso da lui proposti, Schrems aveva contestato, innanzitutto, un impiego su larga scala delle CCS in quanto non era previsto alcun rimedio giurisdizionale usufruibile dall'interessato del trattamento per tutelare i propri dati. Inoltre, criticava il fatto che i propri dati personali trattati da *Facebook*, così come quelli dei milioni di utenti europei, venivano messi a disposizione, con diverse modalità, delle autorità governative statunitensi, alle quali spettava la facoltà di condurre operazioni di spionaggio su larga scala in maniera praticamente incontrollata[62]. Alla luce di questo, egli chiedeva al Commissario irlandese di proibire o sospendere il trasferimento dei dati personali verso gli USA sulla base delle clausole. Il *Data Protection Commissioner*, condividendo le questioni sollevate da Schrems, dalle quali erano nati dubbi circa la validità della decisione della Commissione n. 2010/87/UE sulle clausole contrattuali standard[63], portò la questione innanzi alla *High Court* irlandese.

[60] *Ibid.*, considerando 108.
[61] *Ibid.*, considerando 114.
[62] I. OLDANI, *The future of data transfer rules in the aftermath of Schrems II*, in *SIDIBlog*, 2020.
[63] Decisione della Commissione (UE) n. 2010/87 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 (GU L 39/2010).

Quest'ultima, in considerazione della struttura dell'ordinamento giuridico degli Stati Uniti, che concedeva una serie di ampi poteri ai servizi segreti quali CIA e NSA che si riversavano nel diritto di operare programmi di sorveglianza di massa sui dati personali dei cittadini, ha ritenuto fondati i dubbi sollevati dal Commissario, essendo tali programmi incompatibili con gli artt. 7, 8, 47 e 52 della Carta dei Diritti Fondamentali dell'Unione[64]. Le clausole contrattuali non risultavano essere uno strumento idoneo per limitare l'operato delle autorità statunitensi in quanto conferivano agli utenti dei meri diritti contrattuali esercitabili nei confronti dell'esportatore e dell'importatore di dati. La *High Court* ha quindi sottoposto una serie di questioni pregiudiziali alla Corte di Giustizia dell'UE inerenti alla validità della decisione riguardante le CCS.

Due sono state le questioni esaminate in via preliminare dalla CGUE, ovvero «la delimitazione della portata applicativa e interpretativa del Regolamento n. 2016/679» e la definizione del livello di adeguatezza previsto dall'art. 46 della normativa «nel contesto di una trasmissione di informazioni personali, attuata sulla base di clausole contrattuali tipo»[65]. Nonostante si tratti di questioni che non riguardano direttamente il tema centrale dell'articolo, esse sono fondamentali al fine di comprendere l'evoluzione delle CCS alla luce dell'accesso generalizzato ai dati personali da parte delle autorità pubbliche dello Stato terzo ove i dati vengono importati.

Per quanto concerne il primo aspetto, la Corte si è soffermata sull'art. 2 del Regolamento il quale, al paragrafo 1, definisce l'ambito di applicazione della disciplina e, al paragrafo 2, prevede le eccezioni a questo[66]. La Corte ha stabilito che il trasferimento dei dati operato dalla filiale di *Facebook* irlandese alla casa madre statunitense, in quanto classificabile come attività realizzata per scopi commerciali, era soggetto all'applicazione del Regolamento e non rientrava nelle eccezioni previste dall'art. 2, para. 2[67]. Ciò nonostante, il flusso transeuropeo dei dati per fini commerciali avrebbe potuto successivamente costituire oggetto di trattamento da parte delle autorità dello Stato terzo per scopi di sicurezza o difesa nazionale[68]. La Corte, dopo aver definito l'ambito di applicazione del Regolamento, ha stabilito che questo doveva

[64] M. NINO, *La sentenza Schrems II della Corte di giustizia UE*, *cit.*, p. 743.
[65] *Ibidem*.
[66] Art. 2, para. 1, 2, Regolamento (UE) n. 2016/679, *cit.*: «1. Il 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».
[67] CGUE, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems*, *cit.*, punto 85.
[68] *Ibid.*, punti 86, 88-89.

necessariamente essere interpretato alla luce della Carta dei Diritti Fondamentali dell'Unione europea, rafforzando il regime di tutela dell'ambito della protezione dei dati personali[69].

Per quanto concerne il secondo aspetto, inerente alla definizione del regime di tutela applicabile alle clausole contrattuali standard, la CGUE ha affermato che questo si configura alle medesime condizioni previste nel caso *Schrems I* per la decisione di adeguatezza e, pertanto, qualora l'ordinamento dello Stato terzo destinatario del trasferimento preveda una tutela dei dati personali equivalente a quella dell'Unione[70]. La Corte ha creato, in questa maniera, un unico livello di tutela in materia di protezione dei dati personali applicabile sia per l'istituto della decisione di adeguatezza che per le clausole contrattuali tipo[71], richiedendo, per il rispetto di tale standard, la previsione di garanzie adeguate, diritti azionabili per il singolo e mezzi di ricorso effettivi[72]. Alla luce della *ratio* comune delle norme di cui al Capo V del Regolamento, ovvero quella di «assicurare la continuità del livello di protezione delle persone garantito dal regolamento»[73], l'esportatore deve prendere in considerazione due elementi al fine di effettuare la valutazione sulla effettiva validità delle clausole nel Paese terzo in cui è stabilito. Il primo riguarda la tutela prevista dalle CCS in capo al soggetto interessato. Il secondo concerne la disciplina dello Stato in cui i dati vengono importati in merito di accesso agli stessi da parte delle autorità pubbliche. Al fine di operare tale valutazione assumono rilevanza gli elementi indicati dall'art. 45 RGDP in relazione alla decisione di adeguatezza. Tuttavia, al contrario della decisione di adeguatezza, per la quale questa è effettuata dalla Commissione, per le CCS sono gli esportatori, in *primis*, e le autorità di controllo nazionali, in *secundis*, a dover compiere tale valutazione.

La Corte si è successivamente focalizzata sulla validità della decisione (UE) n. 2010/87 in relazione agli artt. 7, 8, 47 e 52 della Carta di Nizza[74]. La CGUE ha innanzitutto osservato che la natura dell'istituto previsto dall'art. 46 del Regolamento fa sì che le clausole producano effetti solamente nei confronti delle parti contrattuali, ovvero l'esportatore dei dati stabilito nell'Unione e il destinatario dei dati stabilito in un Paese terzo[75]. Rimangono quindi escluse dall'ambito di applicazione delle stesse, non essendo parti contrattuali, le autorità pubbliche dello Stato terzo, che non sono vincolate al rispetto di quanto in esse previsto. La Corte ha individuato due possibili situazioni che si possono verificare a fronte della natura delle clausole a seconda dello Stato di diritto e delle prassi vigenti nel Paese terzo ove ha sede l'importatore

[69] *Ibid.*, punto 89.
[70] CGUE, *Maximillian Schrems c. Data Protection Commissioner*, *cit.*, punti 94-95.
[71] K. IRON, *Schrems II and Surveillance: Third Countries' National Security Powers in the Purview of EU Law*, in *European Law Blog*, 2020.
[72] CGUE, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems*, *cit.*, punti 102-103.
[73] C. CELLERINO, *Trasferimenti internazionali di dati personali e clausole contrattuali tipo dopo Schrems II*, in *Diritto dell'Unione Europea*, n. 2, 2021, p. 362.
[74] I. OLDANI, *The future of data transfer rules in the aftermath of Schrems II*, *cit.*
[75] CGUE, *Data Protection Commissioner c. Facebook Ireland Limited, Maximillian Schrems*, *cit.*, punto 125.

di dati. In un primo scenario il destinatario è in grado di assicurare la protezione dei dati sulla base delle clausole tipo mentre, al contrario, in un secondo scenario, la normativa dello Stato terzo pregiudica, indirettamente, l'applicazione delle CCS. Secondo la Corte una legislazione nazionale che consenta l'accesso ai dati da parte delle autorità pubbliche costituisce una grave ingerenza nei diritti dei soggetti interessati, con il rischio di grave pregiudizio per la validità delle clausole[76].

Pertanto, la CGUE si è chiesta se una decisione della Commissione vertente sulle clausole contrattuali tipo sia invalida nel caso in cui difetti delle garanzie opponibili alle autorità pubbliche degli Stati terzi verso i quali i dati personali sono trasferiti sulla base delle clausole[77]. La Corte innanzitutto ha rilevato come detta decisione si distingua nettamente da una decisione di adeguatezza «la quale mira, in esito a un esame della normativa del Paese terzo interessato che tenga conto, in particolare, della legislazione pertinente in materia di sicurezza nazionale e di accesso delle autorità pubbliche ai dati personali, a constatare con effetto vincolante che un Paese terzo […] garantisce un livello di protezione adeguato e che, pertanto, l'accesso a tali dati da parte delle autorità pubbliche del suddetto Paese non osta ai trasferimenti di dati verso lo stesso Paese terzo»[78]. Al contrario, una decisione della Commissione che adotta CCS non riguarda direttamente uno specifico Stato terzo e, pertanto, non si può ritenere, in forza del dettato dell'art. 46 RGPD, che la Commissione sia tenuta a procedere, prima dell'adozione della decisione, a una valutazione dell'adeguatezza del livello di protezione dei dati garantito dai Paesi terzi verso i quali i dati potrebbero essere trasferiti in forza delle clausole contenute nella stessa[79]. È l'esportatore di dati stabilito nell'Unione europea a essere tenuto a prevedere garanzie adeguate, compensando alla carenza di protezione dei dati dello Stato terzo importatore, così come disposto sia dai considerando 108 e 114 che dall'art. 46 RGDP. Allo stesso modo, la Corte ha rilevato come sia intrinseco nella natura contrattuale delle clausole tipo il fatto che queste non possano vincolare le autorità pubbliche dei Paesi terzi. Tuttavia, richiedendo gli artt. 7, 8 e 47 della Carta di Nizza che il livello di protezione degli individui garantito dal Regolamento non sia compromesso, appare necessario completare le garanzie contenute nelle clausole da parte degli esportatori di dati con sede in uno Stato membro.

In conclusione, la CGUE ha disposto che le clausole contrattuali standard mirano unicamente a fornire agli esportatori di dati stabiliti nell'Unione garanzie uniformi applicabili nei confronti di tutti gli esportatori stabiliti in Stati terzi. Avendo lo scopo di assicurare la protezione dei dati personali che vengono trasferiti in forza delle stesse, queste richiedono che, in determinate situazioni esistenti nel Paese destinatario, vengano adottate misure supplementari da parte dell'esportatore dei dati al fine di garantire

[76] *Ibid.*, punto 126.
[77] *Ibid.*, punto 127.
[78] *Ibid.*, punto 128.
[79] *Ibid.*, punto 130.

il rispetto del loro livello di protezione[80]. L'onere di verificare caso per caso se la normativa vigente nello Stato ove ha sede l'importatore fornisca una protezione adeguata dei dati personali ivi trasferiti grava sul soggetto esportatore, il quale deve, qualora necessario, adottare garanzie supplementari a quelle previste dalle clausole; nel caso in cui ciò non sia possibile si deve necessariamente sospendere o porre fine al trasferimento. Questo è il caso della normativa di uno Stato terzo che imponga al destinatario dei dati provenienti dell'Unione obblighi contrastanti con le clausole, che mettono in discussione la garanzia contrattuale di un livello di protezione adeguato contro l'accesso ai dati da parte delle autorità pubbliche di detto Paese[81]. Conseguentemente, una decisione contenente CCS non può essere ritenuta invalida per il solo fatto che le clausole nella stessa contenute non vincolino le autorità pubbliche dello Stato importatore di dati.

Pertanto, unicamente tale aspetto non pregiudica di per sé il rispetto delle clausole tipo, il quale dipende, piuttosto, dal contenuto delle garanzie che queste prevedono e dall'esistenza di «meccanismi efficaci che consentano, in pratica, di garantire che sia rispettato il livello di protezione richiesto dal diritto dell'Unione e che i trasferimenti di dati personali, fondati su siffatte clausole, siano sospesi o vietati in caso di violazione di tali clausole o di impossibilità di rispettarle»[82]. Pur non definendo in cosa dovrebbero consistere le garanzie supplementari, la CGUE ha disposto una serie di adempimenti che il responsabile del trattamento è tenuto a effettuare, quali il controllo preliminare sull'adeguatezza del livello di protezione dei dati dello Stato terzo ove ha sede il destinatario del trattamento[83]. Se quest'ultimo soggetto non è stato in grado di assicurare il rispetto delle clausole contrattuali tipo egli ha l'onere darne comunicazione al responsabile del trattamento, il quale è tenuto a sospendere il flusso di dati o a risolvere il contratto. Nonostante la previsione di tali oneri in capo al responsabile, le autorità di controllo nazionali rimangono investite del potere di porre in essere le medesime misure sia ai sensi dell'art. 58, para. 2, del Regolamento che nel caso di inerzia del responsabile o dell'incaricato del trattamento[84]. Nell'ipotesi in cui le autorità garanti nazionali adottino decisioni contrastanti in merito, il Comitato Europeo per la Protezione dei Dati è investito del compito di risolvere la questione[85].

Importatori ed esportatori di dati possono continuare a impiegare le CCS come basi giuridiche per operare il trasferimento transfrontaliero di dati. Tuttavia, queste non costituiscono più, in ragione unicamente del loro impiego, garanzie adeguate. È infatti necessario che l'esportatore effettui una valutazione, alla luce del Paese terzo destinatario dei dati, sull'efficacia delle clausole nel rappresentare

[80] *Ibid.*, punto 133.
[81] *Ibid.*, punto 135.
[82] *Ibid.*, punto 137.
[83] *Ibid.*, punto 142.
[84] *Ibid.*, punto 146.
[85] *Ibid.*, punti 150, 160-161.

garanzie adeguate o sulla necessità di adottare misure supplementari. L'esportatore diventa pertanto «responsabile dell'adeguatezza delle garanzie nel caso concreto»[86].

La pronuncia della CGUE per il caso *Schrems II* fissa importanti principi per quanto concerne il rapporto delle clausole contrattuali standard con l'accesso ai dati personali da parte delle autorità pubbliche dello Stato importatore (che, come già affermato, non sono vincolate dalle clausole). In particolare, la sentenza ruota intorno alle garanzie supplementari che l'esportatore di dati ha l'onere di adottare nel caso in cui tale accesso comprometta i diritti degli individui previsti dagli artt. 7, 8, 47 e 52 della Carta dei Diritti Fondamentali dell'UE. Tuttavia, la Corte non specifica in cosa debbano consistere tali ulteriori garanzie e, secondo parte della dottrina, «*it is clear that such measures will have to be identified on a case-by-case basis with due regard to all the circumstances of the transfer and the law of the third country*»[87].

4. La nuova decisione della Commissione sulle clausole contrattuali standard

Pur non fornendo la sentenza *Schrems II* indicazioni dirette e precise in merito alle nuove garanzie supplementari che l'esportatore di dati stabilito dell'Unione ha l'onere di adottare nel caso in cui, a causa dell'accesso ai dati da parte delle autorità pubbliche del Paese importatore, non sia possibile rispettare le CCS, la Corte fissa importanti principi in materia di accesso ai dati oggetto di trasferimento da parte delle pubbliche autorità degli Stati ove sono stabiliti i destinatari.

La nuova decisione della Commissione sulle clausole contrattuali standard appare accogliere, sia direttamente che indirettamente, i suggerimenti della Corte per evitare che detto accesso determini una violazione delle garanzie previste per il trasferimento e la protezione dei dati sulla base delle stesse. La decisione della Commissione n. 914/2021/UE[88], adottata nel giugno 2021, prevede un nuovo regime di clausole contrattuali tipo, al fine di innovare i modelli esistenti alla luce, da un lato, dei nuovi sviluppi in ambito tecnologico e, dall'altro, dei principi e dei requisiti posti dal Regolamento (UE) n. 2016/679 per il trattamento e il trasferimento dei dati, in relazione alla pronuncia della Corte di Giustizia dell'UE per il caso *Schrems II*.

Prima di procedere con l'analisi nel merito della decisione, con specifico riferimento alla materia dell'accesso ai dati da parte delle autorità governative dello Stato terzo, è opportuno soffermarsi sulle numerose innovazioni apportate dalla stessa.

[86] C. CELLERINO, *Trasferimenti internazionali di dati personali*, *cit.*, p. 365.
[87] M. H. MURPHY, *Assessing the Implications of Schrems II for EU–US Data Flow*, in *International and Comparative Law Quarterly*, n. 1, 2022, p. 259.
[88] Decisione di esecuzione della Commissione (UE) n. 2021/914 del 4 giugno 2021 relativa alle clausole contrattuali tipo per il trasferimento di dati personali verso paesi terzi a norma del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio (GU L 199/31).

Per quanto concerne la struttura delle CCS, per la prima volta sono previste una serie di clausole generali da combinate tra loro, mediante un approccio modulare, in base alle differenti tipologie di trasferimento e alla complessità delle catene di trasferimento moderne. Inoltre, le parti possono optare per il modulo più appropriato al caso concreto «in modo da adattare gli obblighi derivanti dalle clausole contrattuali tipo al loro ruolo e alle loro responsabilità in relazione al trattamento di dati in questione»[89]. L'obiettivo della decisione n. 914/2021/UE è quello, da un lato, di facilitare i trasferimenti transfrontalieri di dati e, dall'altro, di assicurare garanzie ai dati personali oggetto di trasferimento[90]. Pertanto, la *ratio* dell'impostazione del regime contrattuale è quella di adattare le CCS alle operazioni eterogenee che possono essere condotte tra importatore ed esportatore, a seconda dei ruoli che questi rivestono nel trasferimento. I quattro moduli sono dedicati ai trasferimenti che avvengono, come di consueto, tra un esportatore che ha sede in un Paese dell'Unione e un importatore che ha sede in un Paese terzo e, rispettivamente, ai trasferimenti da un responsabile del trattamento[91] verso un altro responsabile, da un responsabile verso un incaricato[92], da un incaricato verso un altro incaricato e da un incaricato verso un responsabile. Gli ultimi due modelli rappresentano delle novità assolute sul piano della disciplina europea in quanto, per la prima volta, vengono presi in considerazione dalla Commissione dei trasferimenti tra due incaricati del trattamento e da un incaricato localizzato nell'UE a un responsabile localizzato in uno Stato terzo. Nonostante l'approccio innovativo e flessibile della struttura delle clausole, questa non è esente da criticità dettate dalla possibilità di interfacciare diversi moduli contrattuali all'interno di uno stesso modello generale.

Ulteriore importante novità è rappresentata dall'ambito di applicazione della decisione. L'art. 1 della stessa dispone che le clausole contrattuali standard ivi previste sono considerate in grado di fornire garanzie adeguate ai sensi dell'art. 46 RGPD per i trasferimenti dei dati operati da un esportatore di dati nei cui confronti trova applicazione il Regolamento (UE) 2016/679 a un importatore nei cui confronti detta normativa non trova applicazione. Ciò significa che le CCS devono essere adottate solamente quando il Regolamento non è direttamente applicabile all'importatore. Di conseguenza, i meccanismi per operare i trasferimenti di dati al di fuori dell'Unione europea possono non essere necessari quando i dati sono trasferiti a un soggetto le cui attività rientrano nell'art. 3, para. 2, del Regolamento (UE) 679/2016. Questa

[89] *Ibid*, considerando 10.
[90] *Ibid.*, considerando 3, 5.
[91] L'art. 4 del Regolamento (UE) 2016/679 identifica il responsabile del trattamento nella «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri».
[92] L'art. 4 del Regolamento (UE) 2016/679 identifica l'incaricato del trattamento nella «persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del [responsabile] del trattamento».

previsione, insieme all'approccio modulare delle clausole tipo, «*allows to cater any kind of data transfer between parties, despite of their data processing role or place of establishment*»[93].

Inoltre, vi è la possibilità che più di due parti possano «*adhere or accede to a single set of contractual clauses, potentially limiting the number of separate contracts companies must sign when onboarding new vendors or service providers, currently an onerous task*»[94]. Le nuove clausole contrattuali standard consentono a più esportatori di dati di stipulare contratti (ad esempio, all'interno di gruppi societari) e a nuove parti di aderire a contratti già stipulati mediante la clausola 7. Quest'ultima è una clausola facoltativa che consente a terzi che non sono ancora parti del contratto di aderirvi, senza dover così concludere contratti separati con le altre parti. Questa innovazione mostra la flessibilità del nuovo regime di clausole contenuto nella decisione n. 914/2021/UE.

In conformità a quanto affermato nella sentenza *Schrems II*, è previsto che gli importatori di dati redigano una valutazione d'impatto del trasferimento degli stessi e la rendano disponibile all'autorità di controllo competente qualora questa lo richieda. La valutazione dovrebbe prendere in considerazione diversi fattori. Ad esempio, se le leggi dello Stato terzo in cui i dati vengono importati potrebbero essere in conflitto con le clausole o con il RGPD oppure se sono necessarie ulteriori garanzie per incrementare il livello di protezione dei dati personali. Con riguardo all'accesso ai dati da parte delle autorità governative del Paese ove i dati vengono importati, il destinatario degli stessi ha l'onere di dare contezza della possibilità di tale accesso e a quali condizioni[95]. La valutazione deve essere aggiornata costantemente in base alle modifiche legislative e di prassi in materia operate dallo Stato ove i dati vengono importati.

Un elenco di misure tecniche e organizzative necessarie per assicurare un adeguato livello di protezione dei dati personali una volta trasferiti è fornito all'allegato II della decisione, il quale prevede una serie di misure idonee a garantire la sicurezza dei dati personali. In particolare, questo fa riferimento a certificazioni che attestino un adeguato livello di sicurezza dell'importatore, la descrizione in dettaglio della natura, dello scopo e del contesto del trattamento dei dati, nonché dei rischi che questo comporta con riguardo ai diritti e alle libertà degli individui i cui dati sono trasferiti.

Per quanto concerne specificatamente l'accesso ai dati da parte delle autorità governative dello Stato ove i dati vengono importati, la nuova decisione della Commissione recepisce i principi posti della CGUE nella pronuncia del 2020.

Il tema viene indirizzato, innanzitutto, in una serie di considerando della decisione che stabiliscono come l'importatore dei dati debba comportarsi nel caso in cui la legislazione nazionale del Paese ove ha sede gli

[93] M. C. COMPAGNUCCI, M. ABOY, T. MISSEN, *Cross-Border Transfers of Personal Data after Schrems II: Supplementary Measures and New Standard Contractual Clauses (SCCs)*, in *Nordic Journal of European Law*, n. 2, 2021, p. 8.
[94] C. FENNESSY, *New EU SCCs: a modernized approach*, in *International Association of Privacy Professionals*, 2020.
[95] C. FENNESSY, *Data transfers: questions and answers abound, yet solutions elude*, in *International Association of Privacy Professionals*, 2021.

impedisca di rispettare le clausole a causa della richiesta di accesso ai dati da parte delle autorità governative. È previsto, al considerando 17, che le clausole dispongano che sull'importatore e sull'esportatore di dati gravi l'obbligo di dimostrare il rispetto delle clausole alle quali si vincolano al fine di operare il trasferimento[96]. Da un lato, l'importatore deve informare l'esportatore nel caso in cui non sia in grado di rispettare le clausole e, dall'altro, l'esportatore, nei casi di loro violazione di particolare gravità, ha l'obbligo di sospendere il trasferimento dei dati. Il considerando effettua un primo riferimento generico alla legislazione dello Stato terzo ove vengono importati i dati, disponendo che «si dovrebbero applicare norme specifiche qualora la legislazione locale incida sul rispetto delle clausole»[97]. È sicuramente possibile ricomprendere, all'interno di detta legislazione, le norme che regolamentano l'accesso ai dati da parte delle autorità governative del Paese verso cui i dati vengono importati. Nel considerando successivo si trova, infatti, un primo puntuale riferimento al collegamento dell'accesso ai dati da parte delle autorità pubbliche e come questo possa pregiudicare il rispetto delle CCS. Questo dispone che le clausole debbano prevedere garanzie specifiche «per far fronte a eventuali effetti della legislazione del Paese terzo di destinazione sul rispetto delle clausole da parte dell'importatore, in particolare per quanto riguarda il modo in cui trattare le richieste vincolanti di autorità pubbliche del paese terzo di comunicare i dati personali trasferiti»[98]. È onere delle parti effettuare una valutazione, prima di siglare le clausole, sull'ordinamento giuridico del Paese ove è stabilito l'importatore. Nel caso in cui da questa emerga che la legislazione e le prassi dello Stato terzo impedirebbero all'esportatore di rispettare le CCS, le parti devono astenersi dal concludere il contratto[99]. Al fine di effettuare detta valutazione, il considerando 20 precisa che possono essere presi in considerazione elementi di varia natura, quali le informazioni sull'applicazione pratica della normativa (come la giurisprudenza e le relazioni di organismi di vigilanza indipendenti) e la documentazione attinente ai trasferimenti transfrontalieri redatta dall'importatore o dall'esportatore[100]. Nonostante detta valutazione dia esito positivo è possibile che l'importatore, in seguito alla sottoscrizione delle clausole, abbia motivo di ritenere di non essere in grado di rispettarle e, pertanto, deve informare l'esportatore al fine di individuare misure adeguate per fronteggiare la situazione, quali l'adozione di misure supplementari[101]. Fondamentale, in tema di garanzie supplementari, è la collaborazione tra Commissione e Comitato Europeo di Protezione dei Dati. Sia la decisione che l'allegato effettuano una serie di riferimenti specifici volti a incorporare alcune delle garanzie ulteriori previste dal Comitato nelle raccomandazioni. A queste si fa riferimento, ad esempio, nel considerando

[96] Considerando 17, Decisione (UE) n. 2021/914, *cit.*
[97] *Ibidem*.
[98] *Ibid.*, considerando 18.
[99] *Ibid.*, considerando 19.
[100] *Ibid.*, considerando 20.
[101] *Ibid.*, considerando 21.

22, che afferma la necessità, da un lato, che l'importatore notifichi sia all'esportatore che all'interessato la richiesta di accesso ai dati personali da parte di un'autorità governativa del Paese ove ha sede, che, dall'altro, quella di condividere le informazioni inerenti alle richieste, documentandole, a una serie di intervalli di tempo regolari. Ulteriore necessità è quella, facendo seguito a «un riesame della legittimità di una siffatta richiesta a norma della legislazione del Paese di destinazione»[102], di contestare tale richiesta quando sussistano i presupposti per farlo.

Per quanto concerne specificatamente le clausole, appare opportuno soffermarsi sulla sezione III dell'allegato, rubricata «legislazione e prassi locali che incidono sul rispetto delle clausole». La sezione si compone di due clausole, applicabili per ciascuno dei quattro modelli di trasferimento previsti, che recepiscono quanto disposto dai considerando, disciplinando gli obblighi delle parti nel caso di accesso ai dati da parte delle autorità governative dello Stato terzo. In particolare, la clausola 14 prevede l'obbligo delle parti di garantire di non aver motivo di ritenere che «la legislazione e le prassi del Paese terzo di destinazione applicabili al trattamento dei dati personali da parte dell'importatore, compresi eventuali requisiti di comunicazione dei dati personali o misure che autorizzano l'accesso da parte delle autorità pubbliche, impediscono all'importatore di rispettare gli obblighi che gli incombono a norma delle presenti clausole»[103]. Nell'adempiere a tale obbligo le parti devono aver preso in considerazione una serie di elementi eterogenei elencati dalla clausola stessa. Questi riguardano sia caratteristiche specifiche del trasferimento (quali la lunghezza della catena di trattamento, il numero di soggetti coinvolti, i canali utilizzati per il trasferimento e gli eventuali trasferimenti successivi) che la legislazione e le prassi del Paese di destinazione dei dati che, infine, le garanzie contrattuali, tecniche o organizzative predisposte per integrare le garanzie delle CCS[104]. Nel caso in cui una modifica normativa o di prassi intervenga nel Paese terzo in cui ha sede l'importatore, tale che quest'ultimo la ritenga in grado di pregiudicare il rispetto delle clausole, egli ha l'onere di informare l'esportatore[105]. In seguito alla notifica, così come anticipato dal considerando 20, le parti individuano le misure supplementari da adottare in modo da garantire il rispetto dei principi previsti dal Regolamento (UE) n. 2016/679[106]. La clausola 15 prevede, infine, che l'importatore debba informare prontamente l'esportatore e, se possibile, anche l'interessato, nel caso in cui riceva una richiesta giuridicamente vincolante da parte di un'autorità pubblica di comunicazione dei dati personali ricevuti o venga a conoscenza di accesso diretto ai dati effettuato da dette autorità[107].

[102] *Ibid.*, considerando 22.
[103] *Ibid.*, clausola 14, lett. a), sezione III, allegato.
[104] *Ibid.*, lett. b).
[105] *Ibid.*, lett. e).
[106] *Ibid.*, lett. f).
[107] *Ibid.*, clausola 15.1, lett. a).

Infine, oltre a dette specifiche previsioni vi è un principio che è stato introdotto dalla decisione e che, seppur in maniera indiretta, è volto a fornire una maggiore tutela dei diritti degli interessati contro l'intrusione delle autorità governative degli Stati terzi ove i dati vengono importati: il principio di *accountability*. Il principio di responsabilizzazione delle parti contrattuali, che si trova nel RGPD in varie declinazioni, non solo vincola importatore ed esportatore di dati ma «dovrebbe anche guidarne le scelte strategiche verso la massima tutela dei diritti fondamentali»[108]. L'introduzione di questo principio nella decisione vuole cercare di evitare ogni tipo di approccio puramente formale al rispetto delle CCS.

5. Conclusioni

Il presente articolo si è occupato di fornire una disamina dell'evoluzione della decisione di adeguatezza e delle clausole contrattuali tipo con specifico riferimento all'accesso ai dati personali da parte delle autorità governative degli Stati terzi. A tal fine è stata effettuata un'analisi delle storiche sentenze *Schrems I* e *Schrems II* nella parte in cui hanno trattato, sia direttamente che indirettamente, il tema. Lo studio ha mostrato come l'accesso ai dati personali da parte delle autorità pubbliche dei Paesi terzi ove i dati vengono importati sia estremamente complesso da bilanciare con le esigenze di tutela dei diritti dei soggetti interessati a causa dei numerosi ed eterogenei interessi che entrano in gioco. L'equilibrio tra l'incremento del flusso transfrontaliero di dati e la necessità di tutela dei diritti è precario. Nonostante la spinta alle modifiche legislative e di prassi in tema di trasferimenti transfrontalieri di dati oltre il territorio dell'Unione avvenga principalmente sul piano delle garanzie dei soggetti interessati al trasferimento, gli interessi economici dell'Unione continuano a essere in grado di influenzare le modalità mediante le quali i trasferimenti avvengono, soprattutto con riguardo alla decisione di adeguatezza. Anche le clausole contrattuali standard risentono fortemente di questa costante tensione, tanto che la nuova decisione della Commissione ha cercato di rispondere alle preoccupazioni della CGUE con riguardo all'accesso ai dati da parte delle autorità pubbliche. Il vaglio della Corte in merito all'idoneità della decisione (UE) n. 2010/87 ha mostrato la necessità di predisporre clausole *ad hoc* che disciplinino la richiesta di accesso ai dati personali trasferiti da parte delle autorità pubbliche dello Stato terzo. L'analisi della nuova decisione della Commissione sulle CCS ha evidenziato come effettivamente sia stata introdotta una previsione di questo tipo. A tal fine è stata disposta una maggiore responsabilizzazione dei soggetti che operano il trasferimento e il trattamento dei dati; responsabilizzazione che dovrebbe guidarne le scelte strategiche verso la massima tutela dei diritti fondamentali. Tuttavia, occorrerà valutare se, nel corso dell'applicazione pratica del nuovo sistema di CCS, si assisterà a un effettivo rispetto delle tutele previste nei confronti dell'interessato durante tutta la fase del trasferimento e del trattamento dei dati personali.

[108] C. CELLERINO, *Trasferimenti internazionali di dati personali*, *cit.*, p. 366.

Proprio in relazione al tema dell'accesso ai dati personali da parte delle autorità pubbliche, le recenti conclusioni dell'avvocato generale nella causa *Ligue des droits humains v. Conseil des Ministres* mettono in luce come queste costituiscano ingerenze sia nella vita privata degli individui che nel diritto fondamentale alla protezione dei dati personali[109]. Pur non riguardando il caso direttamente né la decisione di adeguatezza né le clausole contrattuali standard, è comunque utile per fornire ulteriori spunti per l'interpretazione delle clausole tipo analizzate, in modo da garantire il rispetto del contenuto essenziale dei diritti alla vita privata e alla protezione dei dati personali[110].

Appare quindi come l'evoluzione della normativa inerente ai trasferimenti transfrontalieri di dati sia arrivata a un punto di equilibrio per quanto concerne il delicato bilanciamento tra all'accesso ai dati personali da parte delle autorità governative ove i dati vengono importati e la tutela dei diritti dei soggetti interessati. Equilibrio che, tuttavia, risulta estremamente precario nella prassi applicativa sia della decisione di adeguatezza, la cui adozione è spesso guidata da interessi diversi rispetto a quelli di tutela dei dati personali, che, a maggior ragione, delle nuove CCS, la cui efficacia sarà da valutarsi nel corso del tempo.

[109] CGUE, causa pendente C-817/19, *Ligue des droits humains v. Conseil des Ministres*.
[110] *Ibid.*, conclusioni dell'Avvocato generale Giovanni Pitruzzella del 27 gennaio 2022.