Università degli Studi di Padova

Dipartimento di Diritto Pubblico, Internazionale e Comunitario

Corso di Laurea in Diritto e Tecnologia

a.a. 2022/2023

Il quadro USA – UE per la protezione dei dati personali: tutele e prospettive future date dal Data Privacy Framework

Relatore: Chiar.mo Prof. Andrea Pin

Studente: Vanessa Maria Cunico
Matricola: 2014233

Anno accademico 2022-2023

INDICE

Abastract

L'elaborato si prefigge l'obiettivo di esaminare in dettaglio le questioni più delicate concernenti il flusso transatlantico dei dati, un'attività ormai consolidata nel contesto quotidiano. Pertanto si propone di mettere in luce le differenze sostanziali che intercorrono tra i due sistemi a confronto, differenze dovute a una diversa identità storico-giuridica. Inizialmente, attraverso un primo confronto, si analizzerà la concezione stessa del dato personale nelle due superpotenze, evidenziando le peculiarità proprie di ciascun contesto. Successivamente sarà proposta una riflessione sulla natura dicotomica del dato stesso e sulle ragioni giuridiche e le ragioni economiche che da un lato lo vedono come *elemento atomico del "corpo elettronico",* quindi come un elemento intimamente connesso all'individuo cui protezione, sancita all'interno della Carta di Nizza , è finalizzata ad un controllo libero e consapevole di ciò che lo riguarda, dall'altra le ragioni dell'economia che vedono il dato come risorsa economica di primaria importanza, attribuendogli quasi un valore patrimoniale, fungendo da moneta per il consumatore e fonte di profitto per l'azienda. La trattazione, proseguirà con l'analisi delle vicende giurisprudenziali più significative in materia, comunemente note come Schrems I e II per comprendere al meglio quali siano stati empiricamente gli elementi che hanno fatto venir meno le decisioni di adeguatezza, rispettivamente "*Safe Harbor*" e "*Privacy Shield*". Infine, con la consapevolezza delle criticità presentate nei primi capitoli, sarà analizzato l'attuale accordo in materia entrato in vigore il 10 luglio del 2023, il "Data Privacy Framework", individuandone i punti chiave mettendo in evidenzia le peculiarità che lo differenziano dai suoi predecessori e le prospettive future in termini di tutele per i cittadini e adempimenti per le imprese.

INTRODUZIONE

Il diritto alla privacy[1], nato nel contesto statunitense come "*right to be let alone*[2]", è stato successivamente accolto e rielaborato in Europa integrando la sua componente relazionale sulla base dell'identità del vecchio continente. Di conseguenza questo diritto ha assunto una nuova accezione, privacy quale libera determinazione delle modalità di costruzione del sé, nella sua dimensione sociale[3]. Nel contesto europeo questa transizione dalla tradizionale "riservatezza" alla più contemporanea protezione dei dati personali, come autonomo diritto fondamentale al controllo delle informazioni in cui si esprime il sé[4], è sancita dalla Carta di Nizza agli articoli 7 – 8. Pertanto si è osservata un'evoluzione del tradizionale *ius excludendi alios*, verso la conquista di una dimensione attiva, di tutela della proiezione sociale della persona, all'insegna dell'autodeterminazione informativa; principio in base al quale spetta al singolo decidere se e in quali termini rendere noti certi aspetti privati della propria vita [5].

Di diverso pensiero sono gli Stati Uniti, ove nei rapporti orizzontali, la privacy è prevalentemente intesa come un'appendice alla materia consumeristica, in cui la tutela dei dati funge solo da supporto alla protezione del consumatore; si configura pertanto un approccio utilitaristico e settoriale, dal momento che non vi è una singola autorità federale designata alla protezione dei dati, ma una serie di autorità differenti a seconda del tipo di dati e del loro utilizzo, come ad esempio la stessa - *Federal Trade Commission.* Osservando nello specifico il suo ruolo con riguardo alla protezione dati, il suo fine è quello di sventare il pericolo di "*una sorveglianza commerciale*" originabile dalla raccolta indiscriminata da parte delle aziende dei dati personali del *consumer;* tale *sorveglianza* è intesa come la raccolta e l'analisi di dati sulle persone, con il fine di trarne profitto attraverso pratiche commerciali ingannevoli o discriminatorie, quali potrebbero prestarsi ad essere tutte le forme di condizionamento indebito, tali da indurlo ad assumere una decisione che altrimenti non avrebbe assunto

Data la delicatezza dell'argomento e la diversità di vedute tra i due sistemi che vede, da un lato la tutela della libertà di scelta del *data subject*, aspetto chiave in un ordinamento rappresentate *della cultura del consenso,* necessario anche solo per la raccolta, dall'altro la tutela del *consumer* da

[1] Il diritto alla privacy compare per la prima volta nel 1890, all'interno di un articolo pubblicato sulla rivista Harvard Law Review, nella sua prima definizione ossia *right to be let alone*: diritto di esser lasciato soli. Questa definizione che adotta le logiche del recinto, c.d. *ius excludendi alios*, aveva effetto nei rapporti orizzontali conferendo al proprietario la facoltà di opporsi ad ogni ingerenza da parte dei terzi, vista come un'intrusione nella "sua proprietà".
[2] S. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, No. 5, 1890, pp. 193-220
[3] C. D'Cunha, *Idee di Giovanni Buttarelli, trascritte da Christian D'Cunha*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019, reperibile al *link*: https://www.garanteprivacy.it/documents/10160/0/Privacy+2030+-+Un+manifesto+per+il+nostro+futuro+-+Volume.pdf/8a243e2f-53e9-8dfa-a3be- 0e80347499d3?version=2.1, pag 4
[4] S. Rodotà, *Tecnologie e diritti*, Bologna, 1995, p.23
[5] Ivi, 6

pratiche commerciali scorrette in un contesto in cui la raccolta può esser indiscriminata dal momento che si configura un trattamento solo con l'effettivo impiego dei dati, risulta fondamentale che nel flusso transatlantico dei dati vi sia una regolamentazione tale da far valere sia le ragioni giuridiche e le garanzie sancite nella Carta dei diritti fondamentali a tutela dell'individuo, sia le ragioni economiche che vedono il trattamento dei dati come azione portante nell'economia odierna a supporto dei modelli di *business* contemporanei.

Tenendo fede a quanto premesso, nel primo capitolo saranno analizzati gli interessi perseguiti dagli Stati a confronto e le rispettive tutele adottate da quest'ultimi in risposta all'avanzamento del progresso tecnologico, per poi proseguire con una considerazione sulle ragioni a presidio della necessità di mantenere un controllo sui propri dati in quanto strettamente connessi ad un'espressione del libero agire dell'individuo e dunque a presidio di tutte quelle libertà fondamentali sancite nella Costituzione. In modo particolare l'elaborato proporrà anche una riflessione sulla natura dicotomica del dato: il dato come estrinsecazione dell'i*o* e il dato come oggetto di valore economico.

In questo rapporto binario, da un lato il dato è elemento atomico del *corpo elettronico* di quell'*io* virtuale che si viene a creare nel momento in cui il vivere *online* permea sempre di più l'esistenza di ciascuno, dando luogo ad una *persona virtuale* che altro non è che la trasposizione di ciò che la persona è nel mondo. Tuttavia, tale proiezione, risultante dall'elaborazione dei dati raccolti, rende il soggetto conoscibile ad enti pubblici e privati, sulla base dei soli dati su di lui raccolti e trattati. In quest'ottica il rischio è di finire chiuso in quel che si suole definire un "profilo tipo", ponendo il soggetto stesso in una potenziale condizione di pericolo in termini di discriminazione, accesso all'informazione e libertà simili. Per questo nasce l'invocazione di un *habeas data*, ossia un diritto di controllo sulla propria identità digitale, la propria rappresentazione sociale nella dimensione della rete: si tratta di un aspetto chiave che ad oggi nel continente europeo perseguito grazie alla cultura del consenso e alla tutela della figura dell'interessato che in quanto tale è titolare di diritti, i cc. dd. diritti dell'interessato ex art. 15-22 Regolamento 2016/679.

Successivamente, sempre con riferimento alla natura dicotomica del dato, in una chiave di lettura più economica sarà passato in rassegna l'aspetto più consumeristico della questione. Difatti, guardando alle ragioni dell'economia, il trasferimento dati verso paesi terzi è oggigiorno un'azione di prassi quotidiana e di fondamentale importanza per molte realtà aziendali. Negli ultimi anni si sta assistendo ad una crescita esponenziale delle cosiddette *aziende-piattaforma*[6], ossia imprese multinazionali locate in diversi paesi, interconnesse tra loro ed in grado di trasferire le varie

[6] L'azienda-piattaforma è: "un nuovo modello di business che usa la tecnologia per connettere persone, organizzazioni e risorse in un ecosistema interattivo in cui possono essere create e scambiate incredibili quantità di valore".
M. Minghetti, *l'era delle aziende piattaforma*, Sole 24 Ore, 2016, disponibile su:
https://marcominghetti.nova100.ilsole24ore.com/2016/07/18/era-delle-aziende-piattaforma/

informazioni con lo scopo di utilizzare i dati degli utenti per massimizzare i ricavi, ad esempio attraverso l'offerta di annunci pubblicitari in grado di attrarre maggiore attenzione. La trattazione proseguirà al secondo capitolo, guardando alla giurisprudenza comunitaria in materia, attraverso un'analisi della serie di sentenze Schrems che hanno portato all'annullamento, prima, del "*Safe Harbor*" e successivamente del "*Privacy Shield*". Saranno oggetto di indagine le disomogeneità tra i due sistemi. Dall'indagine di queste sentenze sarà possibile comprendere quali siano gli strumenti normativi e gli adempimenti necessari per il trasferimento dati Oltreoceano, quale sia il ruolo delle Autorità indipendenti nell'attività di supervisione e nella definizione di paese sicuro. Infine, all'interno dell'ultimo capitolo, dopo aver compreso nel corso della trattazione l'importanza di riuscire a bilanciare, da un lato, le ragioni dell'economia che da questo traffico di dati ne trae profitto, dall'altro, le ragioni giuridiche, che antepongono ai fini di lucro la protezione della persona, del suo diritto ad autodeterminarsi[7], sarà analizzato il più recente quadro con gli Stati Uniti, osservando i punti chiave e le garanzie promosse dalla decisione approvata in data 10 Luglio 2023: *Data Privacy Framework* USA – UE.

.

[7] Il diritto alla protezione dei dati personali, estende la tutela dell'individuo non solo alla sfera della vita privata, ma anche alle relazioni sociali, così garantendo l'autodeterminazione decisionale e il controllo sulla circolazione dei propri dati (espandendosi nel diritto alla protezione dell'identità personale). Tale diritto trae origine dal diritto al rispetto della vita privata e familiare, del domicilio e della corrispondenza. La dignità della persona umana, infatti, è il valore dominante di tutte le carte dei diritti. E' previsto dall'articolo 8 della Convenzione Europea dei Diritti dell'Uomo del 1950 (CEDU) e costituisce un diritto fondamentale dell'individuo.

CAPITOLO I

LE ESIGENZE DI *BUSINESS* E IL TRASFERIMENTO TRANSFRONTALIERO DEI DATI

1. Il confronto tra l'approccio europeo e statunitense in materia di protezione dati: la diversa concezione dell'individuo tra *data subject e consumer*

Oggigiorno nella società dell'informazione, caratterizzata dal c.d. *cyberspazio* e all'interno di un mondo globalizzato in cui opera una "*data economy*[8]", i dati personali circolano di continuo al di là dei confini geografici degli ordinamenti giuridici[9]. Consegue a ciò che la maggior parte degli scambi tra Europa e Stati Uniti siano caratterizzati da un flusso costante di dati personali, tanto da essere definiti "il sangue vitale dell'economia digitale[10]".

Per quanto concerne i due sistemi a confronto, si può notare come vi siano profonde differenze riguardanti questo campo derivanti da una diversa identità storico-giuridica; di conseguenza, i diversi interessi sostenuti in ciascun sistema si traducono in una diversa tutela della persona [11].

Nella concezione europea la tutela del dato personale è un diritto fondamentale sancito all'interno della Carta di Nizza.[12] La tutela non è intesa come la protezione di una mera unità elementare la cui aggregazione conduce ad informazione[13], ma come protezione di quell'informazione che identifica o rende identificabile, direttamente o indirettamente, una persona fisica, il *data subject* cui il Regolamento UE 679/2016 attribuisce specifici diritti[14], in modo tale che sia libero di esercitare qualsivoglia controllo sulle informazioni che lo riguardano.[15] Siffatta visione del dato personale come estrinsecazione di una qualità dell'individuo meritevole di tutela mette in luce l'intimo legame tra la sua concezione e la libertà dell'individuo di autodeterminarsi[16], principio

[8] *La data economy* è un'economia dei dati basata soprattutto sulla capacità, da parte delle imprese, di gestire la quantità crescente di informazioni digitali e grazie alla loro interpretazione corretta aumentano notevolmente i propri profitti.
[9] P. Guarda - G. Bincoletto, *Diritto comparato della privacy e dei dati personali*, Ledizioni, 2023, 131ss.
[10] R. Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, N.Y. Times, 2015, disponibile in: https://www.nytimes.com/2015/10/11/business/international/behind-the-european- privacy-ruling-thats-confounding-silicon-valley.html
[11] P. Schwartz - K. Nikolaus Peifer, *Transatlanti Data Privacy Law,* Georgetown law journal, 2017
[12] Carta dei diritti fondamentali dell'Unione Europea 2000/C 364/01, (2000), Artt. 7 e 8
[13] Nel linguaggio informatico il dato è un'informazione grezza o elementare ed è solitamente costituito da simboli che devono essere elaborati. L'informazione invece, è un elemento che deriva dall'elaborazione di più dati, che permette di venire a conoscenza di qualcosa.
[14] Il Regolamento UE 2016/679 agli articoli 15-22 prevede i diritti che possono esser esercitati dal *data subject,* tra cui il diritto di informazione, accesso, cancellazione dati e revoca del consenso; per l'esercizio di tali diritti l'interessato può rivolgersi direttamente al titolare del trattamento.
[15] Regolamento UE n. 2016/679 articolo 4
[16] In particolare il riferimento è legato al concetto di "autodeterminazione informativa", espresso per la prima volta dalla Corte Costituzionale tedesca nel 1983, considerando questo un principio essenziale per lo sviluppo dell'individuo.

in base al quale spetta al singolo decidere se ed entro quali limiti rendere noti i fatti legati alla propria vita personale, al fine di mantenere un controllo sulle proprie informazioni. Come sottolinea Stefano Rodotà[17] "*la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente, e nelle forme più diverse, dati che la riguardano*[18]".

Inoltre questa attenzione volta alla protezione dei dati funge anche da presidio al principio di libertà personale difatti serve a evitare che la raccolta arbitraria di queste particolari informazioni, si trasformi in uno strumento di pregiudizio contro le persone stesse[19]: "*senza una forte tutela del "corpo elettronico", dell'insieme delle informazioni raccolte sul nostro conto, la stessa libertà personale è in pericolo e si rafforzano le spinte verso la costruzione di una società della sorveglianza, della classificazione, della selezione sociale*".[20]

Se nell'Unione Europea la protezione dei dati personali costituisce un diritto fondamentale, secondo i valori del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza[21].

Negli Stati Uniti, con riguardo alla protezione dati nei rapporti orizzontali[22], a prevalere è la libera circolazione dell'informazione in linea con lo spirito liberalista[23]. Nella nazione epicentro del capitalismo, ove il dato è considerato alla stregua di un bene commerciabile, la sua protezione non è finalizzata alla salvaguardia di un diritto fondamentale, ma alla protezione del consumatore; conseguentemente essendo considerata come un'estensione della tutela dei consumatori[24], la sua disciplina è stata principalmente affidata alla *Federal Trade Commission* [25](FTC). L'approccio statunitense si presta ad essere indubbiamente più efficace e flessibile dinnanzi alle evoluzioni tecnologiche, tuttavia questa propensione a trasformare il dato personale in un bene economico oggetto di scambio, ha come risultato quello di svilirne l'aspetto più intimo ed individuale.

---

[17] Giurista italiano, eletto nel marzo del 1997 presidente dell'organo collegiale del Garante per la protezione dei dati personali, carica che ha mantenuto fino al 2005.
[18] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari 2001, 28-32
[19] S. Rodotà, *Privacy Freedom and Dignity: conferenza internazionale sulla protezione dei dati personali*: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293
[20] Ibidem
[21] Art 2 TUE
[22] Nel contesto statunitense vi è una differenza tra la tutela della privacy tra privati e rispetto al potere pubblico, difatti in quest'ultimo caso esiste un diritto alla privacy che protegge gli individui quando il governo tratta i loro dati personali. Questo si può rinvenire nella costituzione al Quarto Emendamento. Il Quarto Emendamento protegge gli individui da alcuni tipi di raccolta di informazioni personali da parte del governo, è il diritto di essere sicuri contro le perquisizioni di "persone, case, documenti ed effetti" è tutelato sempre in un'ottica di protezione della propria proprietà dalle ingerenze pubbliche.
[23] P. M Schwartz, *Transatlantic Data Privacy Law*, 2017, https://escholarship.org/uc/item/1ws1r1cz, 132-136
[24] B. Saetta, *Protezione dati personali: la privacy negli USA,* disponibile in: https://protezionedatipersonali.it/privacy-negli-usa
[25] *La Federal Trade Commission* è un'agenzia federale che si occupa di far rispettare le leggi antitrust americane e della protezione dei consumatori.

Inoltre rientrando nell'alveo del diritto dei consumatori non contempla i *diritti degli interessati*: ciò significa che non vi è una legge federale che prevede il diritto di accesso, il diritto alla cancellazione e simili, fatte salve alcune eccezioni ad esempio in materia sanitaria.

Pertanto, tale libero scambio dei dati e la mancanza di strumenti di controllo su questi, sebbene possa risultare funzionale al progresso tecnologico, porta con sé l'inevitabile conseguenza di rendere il *consumer* oggetto di un'interferenza costante da parte di date aziende. Ragion per cui solleva notevoli preoccupazioni nei confronti della *FTC* il tema della *sorveglianza commerciale*, attività che la Stessa definisce come la raccolta e l'analisi di dati sulle persone, da parte delle aziende, che acquisendo una conoscenza sempre più profonda delle esigenze e abitudini [26] possono mettere in atto pratiche commerciali poco chiare, se non, ingannevoli volte alla creazione di profitto. [27]

Inoltre, negli Stati Uniti la scelta di tutelare la privacy in maniera settoriale e indiretta porta a una proliferazione di normative che rende estremamente difficile per i cittadini conoscere con precisione i propri diritti. Sebbene ai fini della trattazione sia stata menzionata solo la disciplina della privacy afferente alla *FTC*, la privacy è disciplinata anche altrove: ad esempio, nel settore sanitario esiste la c.d. normativa *Health Insurance Portability and Accountability Act* che regolamenta le informazioni sanitarie utilizzate da ospedali o compagnie assicurative. Si tratta però solo di specifiche normative dedicate ai singoli settori.

Al contrario nel vecchio continente, l'attenzione principale, rivolta all'esigenza di tutelare i diritti fondamentali dei cittadini, le loro libertà e la tutela delle loro informazioni personali, si traduce in un approccio generalista, secondo cui la privacy è tutelata indipendentemente dal settore di applicazione.

1.1 L'*habeas data* nell'era digitale

La rete oggi non rappresenta più solo un mezzo di connessione utile in funzione di supporto alla realtà; piuttosto rappresenterebbe una realtà a sé, uno spazio in cui l'individuo partecipa nella sua dimensione virtuale che altro non è che il risultato del suo modo d'essere nel mondo reale. Il cambio di paradigma dovuto al sempre più comune vivere nella dimensione *online*, al relazionarsi, al lavorare, allo svolgere attività quotidiane, ha come inesorabile rischio quello di ridurre la persona ad oggetto dal quale vengono costantemente estratte tutte le possibili informazioni non solo per finalità di controllo sociale, ma sempre di più per costruire profili ed identità, stabilendo nessi e relazioni,

[26] M.L.G Sakamoto, *International data transfer. An analysis of Schrems cases I and II*, In Seven Editora eBooks. 2023 https://doi.org/10.56238/devopinterscie-092, 5

[27] R. Berti - F. Zumerle, *Privacy negli Usa a che punto sono le prime regole nazionali*, 2022, disponibile in: https://www.agendadigitale.eu/sicurezza/privacy/privacy-negli-usa-a-che-punto-sono-le-prime-regole-nazionali/

soprattutto, per finalità economiche[28]. Per questo motivo, in un momento in cui il rifiuto a fornire le proprie informazioni personali implicherebbe l'esclusione da un numero crescente di processi sociali, acceso all'informazione, fornitura di beni e servizi, [29]le informazioni che danno vita all' "io" virtuale devono sempre esser oggetto di controllo da parte del proprietario, che ha diritto a seguire le proprie informazioni e ad opporsi a forme di ingerenze varie.

Pertanto la rappresentazione sociale del "sé" risultante dalla manipolazione dei dati raccolti, può rivelarsi particolarmente pericolosa e lesiva per l'individuo a causa dell'attitudine dei dati ad esser oggetto di manipolazioni da parte di soggetti pubblici e privati; il che può determinare comportamenti finalizzati alla discriminazione dell'individuo sulla base del profilo d'identità originatosi e alla compromissione di libertà quali quella di espressione, di accesso all'informazione e simili; ragion per cui tali *elementi atomici* che costituiscono il "*corpo elettronico*", i dati, non possono esser trattati come semplici oggetti di scambio[30].

Siffatta attenzione europea a tutelare il dato dal divenire un bene di commercio è messa in luce da questo passaggio, tratto da *la vita e le regole* di Stefano Rodotà: "*i diritti fondamentali si pongono a presidio della vita che in nessuna sua manifestazione può essere attratta nel mondo delle merci*[31]."

Dunque si presta ad essere una prerogativa della politica europea l'evitare che i dati personali vengano trattati alla stregua di qualsiasi bene economico secondo le regole dei mercati, dal momento che ciò andrebbe a costituire una mercificazione di quelle informazioni in cui si esprime la personalità[32]. Pertanto, come è stato autorevolmente sostenuto,[33] è necessario porre delle condizioni affinché si implementino delle garanzie costituzionali adeguate all'era digitale, in cui si riconosca il principio dell'"*habeas data*[34]", finalizzato alla protezione dei dati, alla tutela dinamica della sfera privata e dell'identità garantendo al cittadino di esser libero di esercitare al meglio il diritto all'autodeterminazione informativa.[35]

---

[28] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli, op. cit* 27 ss.
[29] Ibidem
[30] Ibidem
[31] Ibidem
[32] C. D'Cunha, *op cit.,*4
[33] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli, op. cit.,* 30
[34] Nel 1679 venne codificato il principio dell'*habeas corpus,* principio fondamentale a presidio dell'inviolabilità della persona. Oggi nell'era della digitalizzazione, in cui i dati si riflettono come proiezione della persona è necessario ricorrere ad un *habeas data*, alla base del diritto di controllo sui propri dati personali. Dati raccolti, archiviati e conservati da entità di varia natura, pubbliche e private sui quali è urgente, oltre che utile, chiedere la massima trasparenza per evitare violazioni della privacy, intrusioni e abusi vari, tutti resi possibili oggi da tecnologia, sempre più spesso usate per finalità di sorveglianza e controllo.
[35] S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, *op cit.,* 30-32

1.2. L'avvento delle *platfirm* e il modello di *business* basato sull'impiego di dati personali.

Il trasferimento dei dati rappresenta il flusso vitale che alimenta l'ecosistema delle piattaforme digitali, in altre parole può esser inteso come la struttura portante su cui si fondano i modelli di business contemporanei contraddistinti dall'avvento delle "platfirm[36]".

Queste nuove aziende piattaforma, c.d. "*platfirm*", adottano un modello di business basato sullo scambio dei dati con un servizio digitale[37]. Il sinallagma contrattuale che nasce da questo "scambio", talvolta rischia di trarre in inganno l'utente finale che potrebbe fornire un consenso non consapevole quando, non essendo adeguatamente informato delle reali finalità della raccolta, ritenga tale gratuito non consapevole del potenziale valore economico del dato che si presta ad esser un sostituto del corrispettivo monetario. [38] Dunque, tale raccolta di dati, che le aziende ottengono dal proprio bacino di utenti attraverso la navigazione sulle piattaforme digitali, quando finalizzata unicamente alla fornitura del servizio digitale, generalmente trova la base giuridica per giustificarsi nell'esigenza di dare esecuzione al contratto che l'utente perfeziona al momento dell'accettazione dei termini d'uso della piattaforma e, dunque, ex art. 6, paragrafo 1), lettera b) del Regolamento Privacy 2016/679.

Tuttavia quando siffatta raccolta non si limiti solo alla fornitura del servizio digitale, ma sia volta ad ottenere un profitto dal loro trattamento, costituisce una forma di monetizzazione del dato priva della suddetta base giuridica per giustificarsi; quindi si rende necessario un consenso consapevole, libero, informato.[39]

Difatti, le nuove capacità analitiche degli algoritmi, sempre più potenti e meno costose, e quelle di elaborazione, di questa ingente mole di informazioni, sottratte agli utenti, non solo consentono di estrarre conoscenza, ma anche di effettuare valutazioni predittive sui comportamenti degli individui al fine di condizionarne scelte o decisioni utili al profitto.[40] Esempio lampante di quanto affermato, si presta ad essere la vicenda del supermercato statunitense Target[41] che grazie alla profilazione effettuata sui dati di acquisto dei propri consumatori riuscì ad individuare le tendenze e il comportamento di una particolare categoria, nello specifico quella delle donne incinte; cosi , avendo

[36] L'azienda piattaforma è caratterizzata da un nuovo modello di business che prevede la connessione diretta tra consumatore e produttore secondo un approccio "*interaction first*", il quale assume che l'interazione tra consumatori e produttori è il meccanismo principale della creazione e scambio di valore sulla piattaforma.
[37] M. Minghetti, *op cit.*
[38] Ad oggi l'assimilazione dell'atto di consegna dati al concetto di *controprestazione* è ancora incerta dal punto di vista formale, tuttavia essendo una prassi all'ordine del giorno viene data una tutela al consumatore che si trova a fornire i propri dati ai sensi della Direttiva 770/2019 recepita agli artt. 135 ss. del cod. cons.
[39] Garante per la protezione dati personali, *Facebook, i dati personali possono essere corrispettivo di un servizio? Lecito dubitarne*, disponibile in: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575591.
[40] A. Soro, *Un'economia basata sui dati*, intervento, 14 Novembre 2019, disponibile in: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3545472
[41] C. Duhigg, *How companies learn your secrets*, The New York Times Magazine, 2012 disponibile in: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

compreso le loro tendenze, sulla base delle "informazioni catturate" riuscì ad anticipare il bisogno del consumatore finale promuovendo prodotti *ad hoc* secondo le esigenze del caso.

Ciò che può sembrare un vantaggio a favore del cliente in realtà si pone all'interno di un quadro problematico rappresentato dal rischio di discriminazione derivante dalla pubblicità comportamentale[42] a seguito di profilazione. Infatti la particolare configurazione dell'algoritmo di profilazione potrebbe dar luogo ad un effetto discriminatorio in termini di diversificazione di prezzi, per esempio sulla base di status sociali o di presunti interessi, con il rischio che mostri importi particolarmente alti fino a escludere determinati soggetti dall'acquisto di un dato bene o servizio.[43]Analogamente potrebbe poi verificarsi una differenziazione dell'offerta di prodotti o condizioni di acquisto in virtù di una distinzione tra profili originati a seconda della situazione economica individuale, caratteristiche etniche, religiose o di genere[44]. Vi sono quindi varie ipotesi di rischio, tali operazioni di profilazione possono minare la libertà di accesso all'informazione e, di conseguenza, la libertà di scelta, lasciando l'interessato "rinchiuso" nel profilo all'interno del quale è stato classificato.[45]

Spostando l'attenzione invece alle sedi di elaborazione e trattamento dei dati raccolti da parte delle aziende-piattaforma, emerge un ulteriore aspetto significativo e interessante da osservare, ossia il carattere quasi monopolistico esibito dalle piattaforme basate negli Stat Uniti. Tanto è vero che la maggior parte delle piattaforme che vengono utilizzate quotidianamente svolge l'attività di elaborazione dei dati in *server* installati sul territorio statunitense, ad esempio Meta[46]e Google[47]. Questo fatto aggiunge un livello di complessità ulteriore, dal momento che per l'impiego di determinati servizi di uso quotidiano, il trasferimento dati tra le due superpotenze si rivela necessario.

Tuttavia lo scambio di dati non può esser trattato alla stregua dello scambio di beni, in quanto coinvolge l'identità di ogni individuo e quindi la sovranità giuridica legata alla cittadinanza.

Nel contesto europeo il timore di una sorveglianza generale, massiva e indiscriminata perpetrata dalle autorità di *intelligence* statunitensi a danni dei cittadini europei, è da anni causa di

[42] La pubblicità comportamentale si basa sulla personalizzazione dei contenuti, attraverso l'analisi delle informazioni personali degli utenti, e sulla previsione di attitudini comportamentali. Andando ad identificare gli utenti, essa comporta un trattamento di dati personali soggetto alla disciplina privacy.

[43]F. Banterle, *Pubblicità comportamentale, GDPR e rischi di discriminazione in: Società delle tecnologie esponenziali e General Data Protection Regulation: Profili critici nella protezione dei dati*. Milano, Ledizioni, 2018, disponibile in Internet: http://books.openedition.org/ledizioni/3943, 11-34

[44] Ibidem

[45] Ibidem

[46] L'azienda Meta, precedentemente nota come Facebook Inc, dispone di vari server tra cui alcuni locati in territorio europeo; tuttavia il trattamento dei dati carpiti ai cittadini europei è soggetto ad un trasferimento nel territorio statunitense dove sono presenti i server principali.

[47] Anche Google possiede diversi server locati nel territorio europeo, tuttavia quelli principali sono stabiliti negli Stati uniti; tanto che l'impiego di Google Analytics è stato sanzionato dal Garante italiano all'azienda nazionale "Caffeina Media S.r.l" dal momento che le informazioni acquisite con questo strumento e il conseguente trasferimento nel territorio statunitense non garantivano un livello adeguato di protezione dei dati personali degli utenti.

conflitti giudiziari in materia di trasferimento dati. Per tale motivo l'Unione a presidio delle garanzie e diritti dei *data subject* è intervenuta con accordi *ad hoc*, le c.d. decisioni, in modo tale da definire un quadro con gli Stati Uniti che vada a bilanciare i diritti fondamentali sanciti agli artt. 7 e 8 con le esigenze di pubblica sicurezza statunitensi. [48].

1.1.2. L'equazione "dati uguale potere": dalla raccolta di dati alla produzione di profitto

Alla luce di quanto detto precedentemente, il contesto odierno risulta definito dalla logica "dati uguale potere", intendendo con il termine potere quella facoltà di "*raccogliere informazioni sulle persone, costruire inferenze attraverso quelle informazioni e trasformarle in fonte di valore"* sotto forma di profitti commerciali anche in termini di capacità di condizionamento dei comportamenti altrui,[49] secondo il processo anche detto *datificazione*.[50]. Ciò è la ragione per cui l'era contemporanea è anche comunemente nota come "*data driven world*" (*i dati alla guida del mondo)*, in quanto dallo sfruttamento massivo dei dati su varie scale, sia in ambito pubblico che privato, si giunge alle attività di creazione ed elaborazione di modelli in grado di fornire conoscenza e di fungere da supporto principale ai processi decisionali.[51] Pertanto, la peculiare natura del dato ad essere oggetto di manipolazione, oltre all'intrinseca capacità di produrre conoscenza, ha suscitato di un generale timore europeo, nei confronti delle piattaforme statunitensi, dando luogo ad un momento in cui la regolamentazione appare come necessaria per fronteggiare le sfide e le esigenze poste dalla crescita esponenziale dei servizi digitali e dalla concentrazione di potere rappresentata dalle piattaforme digitali statunitensi. [52]

1.3. L'effetto Bruxelles

Con il termine "effetto Bruxelles" si fa riferimento alla capacità unilaterale dell'Unione europea di regolare i mercati globali stabilendo dei modelli normativi in varie materie, tra cui la protezione della dei dati personali, che costringono altri ordinamenti e soprattutto il mondo produttivo globale ad adeguarvisi. Partendo dal presupposto che l'UE sia uno dei più grandi e ricchi mercati di consumo, difficilmente escluso dai rapporti commerciali, consegue che il prezzo per accedere al

[48] P. Darnis, *Le relazioni transatlantiche al tempo del digitale: la questione del trasferimento di dati*, Istituto Affari Internazionali, 2021, 4
[49] C. D'Cunha, *op cit.,* 12ss.
[50] C. Sarra, *Il mondo dato*, Coop. Libraria Editrice Università di Padova, 2019, 13 ss.
[51] Ivi, 33, 34
[52] P. Darnis, *op. cit.,* 4-5

mercato unico molto spesso consista nell'adeguare la condotta e produzione agli standard dell'Unione.[53]

Conseguenza dell'Effetto Bruxelles è l'adozione di regolamenti in stile europeo da parte di ordinamenti stranieri.[54] Questo fenomeno è la ragione per cui il meccanismo che permette il flusso trans-atlantico dei dati vede l'Unione Europea svolgere un ruolo chiave nella definizione delle misure necessarie ed essenziali in protezione dei diritti fondamentali dei suoi cittadini. Di riflesso, all'interno del Regolamento vi è un'importante previsione per il traffico dati dei cittadini europei. All'articolo 3 del Regolamento UE 679/2016 viene trattato l'ambito di applicazione territoriale del medesimo, il quale al secondo paragrafo evidenzia come si debba applicare ogni qualvolta vengano trattati dati di cittadini europei da parte di un titolare che sia stabilito o meno nell'Unione quando[55]:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

L'Unione europea ha dunque adottato un approccio basato sulla geografia che mira a proteggere dai rischi posti dal Paese o dal luogo in cui i dati devono essere trasferiti. Le legislazioni nazionali che seguono l'approccio geografico prevedono vari criteri di ammissibilità dei trasferimenti di dati, primo tra tutti il livello di adeguatezza del Paese in cui i dati saranno esportati.

1.4. Il trasferimento dati verso paesi terzi

Il trasferimento di dati personali è un'attività che avviene quotidianamente per varie finalità, come l'operatività di servizi digitali ad esempio quelli *cloud* o di *social network*, i cui *server* sono tendenzialmente collocati in un luogo diverso rispetto a quello da cui l'utente accede. A livello europeo e di conseguenza anche per tutti quei paesi che desiderano rapportarsi con i dati dei suoi concittadini, questa materia è regolamentata al Capo V del Regolamento 2016/679 specie quando si tratta di trasferimento dati verso paesi terzi e organismi internazionali. L'art. 44 del GDPR apre il Capo V dedicato alle regole sul trasferimento di dati personali al di fuori dell'Unione europea verso un paese terzo o un'organizzazione internazionale. Ai sensi di questa norma i dati personali non

[53] A. Bradford, *The European Union in a globalised world: the Brussels effect*, 2021, 75,79
[54] Ibidem
[55] Regolamento UE 2016/679 articolo 3) par. 2)

possono essere trasferiti a meno che non si rispettino le condizioni previste dal Capo V, in modo da assicurare che il livello di protezione dei dati garantito da esso stesso non venga pregiudicato [56].

1.1.4. L'art 45: la decisione di adeguatezza e la definizione di paese sicuro

Lo strumento che rende possibile il trasferimento dati è innanzitutto la decisione di adeguatezza.

Essa è la prima situazione in cui è consentito il trasferimento di dati al di fuori dell'Unione e si verifica quando il paese terzo garantisce un livello di protezione dei dati equiparabile a quello previsto dal Regolamento [57]. Con il termine "adeguato" si intende che nel paese destinatario la protezione fornita debba sostanzialmente esser equivalente a quella garantita all'interno dell'Unione[58]. Per ottenere la decisione di adeguatezza il paese terzo può chiedere alla Commissione europea di esaminare la propria legislazione[59] . Quindi la decisione di adeguatezza costituisce la prima base giuridica per il trasferimento, dal momento che esclude la necessità di autorizzazioni specifiche per il titolare o il responsabile vista la valutazione per l'adeguatezza da parte della Commissione, esaminati dati aspetti[60]:

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

[56] P. Guarda - G. Bincoletto, *op cit., 133*
[57] B. Saetta, *op cit.*
[58] Paragrafo 74 sentenza Schrems C-362/14
[59] Regolamento UE n. 2016/679 articolo 45
[60] Regolamento UE n. 2016/679 articolo 45 par. 2

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.

Le decisioni di adeguatezza emanate dalla Commissione europea sono vincolanti per i paesi dell'Unione e in base ad esse è ammesso il trasferimento di dati verso il paese indicato. Tali decisioni possono essere modificate, sospese o revocate se risulta che il paese terzo non soddisfa più i criteri necessari.

1.2.4 Le *Standard Contractual Clauses* e le *Biding Corporate Rules*

Il secondo strumento che può esser impiegato al fine di trasferire i dati, nel caso in cui non fosse possibile usufruire della decisione di adeguatezza, è l'impiego delle cosiddette *Standard Contractual Clauses*. Le clausole contrattuali tipo sono dei modelli contrattuali, approvati dalla Commissione europea *ex ante* e validi ai sensi dell'art 46, par. 2), lett. C), che conferiscono delle garanzie pari a quante richieste dal Regolamento tramite cui il titolare o il responsabile del trattamento possono assicurare la conformità del trasferimento dati e legittimare il trasferimento medesimo. Esse sono predisposte in modo tale da garantire la conformità rispetto ai principi generali in materia di trattamento e protezione dei dati personali fin dalla progettazione.

Le *clausole contrattuali tipo* possono essere, principalmente, incorporate nei contratti redatti sia tra due titolari, uno stabilito nell'Unione l'altro sia tra un titolare ed un soggetto semplicemente incaricato del trattamento nel paese terzo. L'esportatore dei dati deve incorporare tali clausole contrattuali in un contratto utilizzato per il trasferimento, in modo tale da garantire che i dati saranno trattati conformemente ai principi stabiliti nel regolamento europeo anche nel Paese terzo di destinazione. Il testo di tali clausole non può essere modificato rispetto a quello reso pubblico dalla Commissione Europea[61].

Un ulteriore strumento è previsto dall'art. 47 e riguarda società facenti parti dello stesso gruppo d'impresa, laddove una di queste si trovi al di fuori dell'Unione Europea. Queste regole consistono in un regolamento interno al gruppo nazionale in materia di privacy, che la capogruppo, stabilita all'interno dell'Unione, adotta attraverso una sua dichiarazione unilaterale creando per tanto un vincolo per le società collegate[62]. In altri termini *le Binding Corporate Rules (BCR)* si concretizzano in un documento contenente una serie di clausole che fissano i principi vincolanti per

[61] B. Saetta, *op cit.*
[62] N. Bernardi, *Privacy. Protezione e trattamento dei dati*, 2019, 306, 311

tutte le società appartenenti allo stesso gruppo.[63] Anche in questo caso le clausole devono essere sottoposte alle autorità di controllo, ma è possibile elaborare clausole sulla base di quelle già esistenti e sulle quali già si siano pronunciati i garanti, in modo da avere sufficiente certezza che siano accolte.[64]

Infine in mancanza di una decisione della Commissione e di uno degli strumenti appena descritti, il Regolamento prevede che il trasferimento dei dati personali possa avvenire sulla base di una deroga previste dall'art 49.

1.3.4 L'art 49: le deroghe che consentono il trasferimento di dati personali verso un paese terzo

Le deroghe sono eccezioni al principio generale secondo cui i dati personali possono essere trasferiti verso paesi terzi soltanto in presenza di adeguate garanzie. Nel contesto del Regolamento 679/2016, in assenza di una decisione della Commissione e delle garanzie precedentemente descritte, il trasferimento dei dati personali può avvenire utilizzando le deroghe previste all'articolo 49 [65].

All'articolo 49 è infatti prevista la possibilità di trasferire dati quando: l'interessato abbia esplicitamente acconsentito, il trasferimento è occasionale e necessario in relazione a un contratto o a un'azione legale, sussistono motivi di rilevante interesse pubblico previsti dal diritto dell'Unione o degli Stati membri o dalle persone aventi un legittimo interesse.

Le deroghe rappresentano delle eccezioni al principio generale che richiede adeguate garanzie nel paese terzo per il trasferimento dei dati personali. Tuttavia, le deroghe devono essere interpretate in maniera restrittiva, considerando che l'interessato deve continuare a beneficiare dei diritti fondamentali e delle garanzie, nonché delle garanzie effettive e attuabili

[63] Ibidem
[64] P. Guarda - G. Bincoletto, *op cit.,* 142,143
[65] Regolamento UE n. 2016/679 articolo 49

CAPITOLO II

LE CRITICITA' NEL RAPPORTO USA – UE: LA GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA

Nel presente capitolo, l'elaborato si pone come obiettivo di condurre un'analisi empirica delle più significative pronunce giurisprudenziali concernenti la tutela dei dati personali. Tali pronunce hanno innegabilmente alterato la dinamica relazionale tra gli Stati Uniti e l'Europa in questa materia. Attraverso un dettagliato esame del *corpus* decisionale noto come "*Schrems*", si intende delineare in maniera esaustiva le lacune e le problematicità riscontrate nelle precedenti decisioni di adeguatezza. Questa analisi è finalizzata a fornire una solida base per una comprensione approfondita del contesto attuale, rappresentato dal *Data Privacy Framework* USA - EU a testimonianza del cambio di paradigma dato dall'avvicinamento del modello statunitense a quello europeo.

2. Maximilian Schrems v. Facebook: la sentenza Schrems I e l'annullamento del *Safe Harbor*

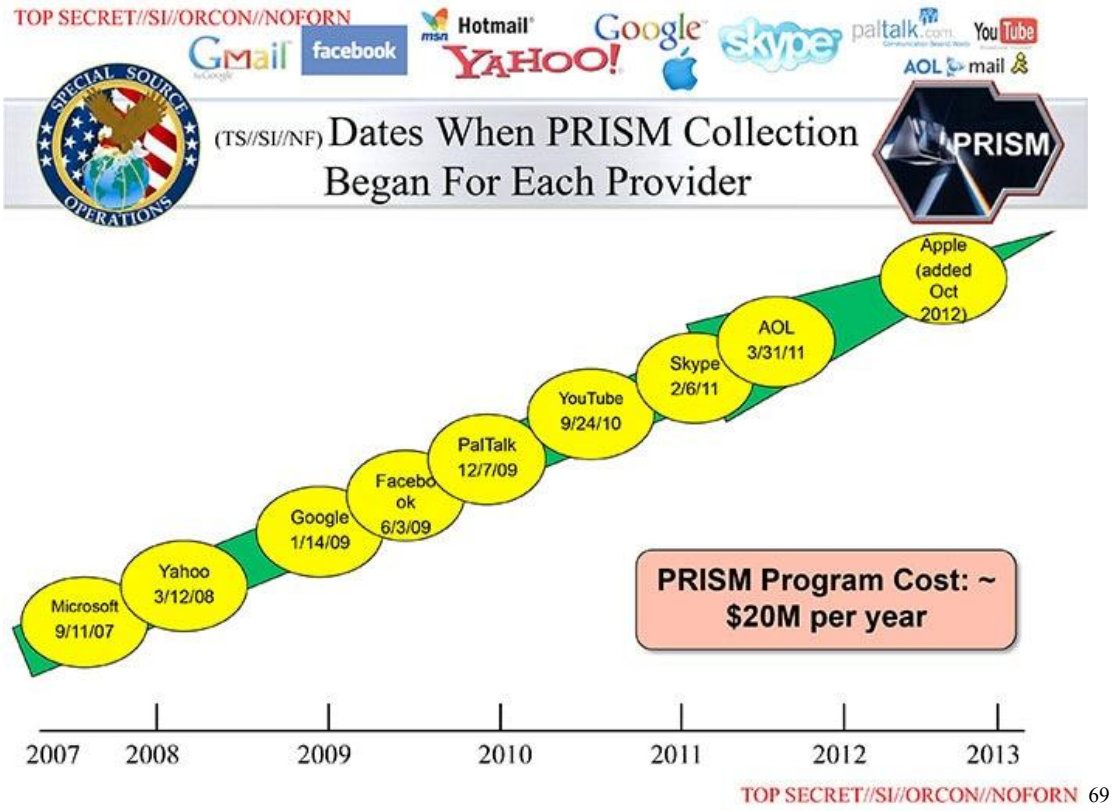
La vicenda giudiziaria che portò ad un susseguirsi di sentenze fondamentali in ambito di trasferimento dati, comunemente note come Schrems I e II, trae origine dalla denuncia presentata dal giovane Maximilian Schrems, cittadino austriaco e attivista per la protezione dei dati personali. La stessa fu presentata alla luce delle rivelazioni di Snowden,[66]le quali sollevarono vari sospetti sul livello di protezione dei dati garantito all'interno dell'ordinamento statunitense. Nelle stesse vennero denunciate le raccolte indiscriminate su larga scala dei dati nonché l'accesso a questi ultimi nei *sever* delle principali *Big tech,* da parte della *national survaillance authority* (NSA*)*. Inoltre, emerse che queste ingerenze, autorizzate da una legge nazionale, il c.d. *FISA*[67]*,* costituivano la base fondamentale del programma di sorveglianza *Prism*[68].

[66] A seguito delle rivelazioni di Snowden, tutto il mondo scopriva che i servizi *di intelligence* statunitensi trattavano enormi quantità di dati anche di individui di altri paesi dando luogo allo scandalo "*Datagate*".

[67] Il FISA, *foreign intelligence surveillance act*, è una legge degli Stati Uniti che si occupa della raccolta di informazioni e sorveglianza delle comunicazioni di individui stranieri all'estero. In particolare la sezione 702 del FISA autorizza il monitoraggio delle comunicazioni elettroniche, mail telefonate etc, di individui stranieri residenti all'estero o che comunicano con cittadini statunitensi al fine di trarre informazioni utili per la sicurezza del paese. Le grandi Big tech, sono soggette al FISA pertanto i dati di un utente possono esser soggetti all'accesso da parte di agenzie governative statunitensi. R. Rhc, *Scopriamo la sorveglianza di massa e il Foreign Intelligence Surveillance Act (FISA) e la sezione 702*, Red Hot Cyber, 2023, disponibile in: https://www.redhotcyber.com/post/foreign-intelligence-surveillance-act-section-702/?utm_content=cmp-true

[68] Il programma PRISM consente all'intelligence statunitense di ottenere da nove società Internet l'accesso a un'ampia gamma di informazioni digitali, tra cui e-mail e dati memorizzati sui server stessi, appartenenti ad individui stranieri che vivono al di fuori degli Stati Uniti. Opera sulla base del Foreign Intelligence Surveillance Act (FISA).
B. Gellman - L. Poitras *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, Washington Post, 2013, disponibile in: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

Attraverso tali rivelazioni il sig. Snowden dichiarò a quali *server* delle *Big tech* avessero accesso le agenzie di *intelligence* e soprattutto da che anno era cominciato il programma *Prism*, da quanto i dati erano conservati, trattati senza che agli interessati fosse stata fornita alcuna informazione.



69

Dall'immagine si può notare come la maggior parte delle aziende coinvolte in questo programma permeino la nostra quotidianità oggi come allora. Attraverso questo programma, l'*NSA* era in grado di accedere direttamente ai *server* delle aziende partecipanti e di ottenere sia le comunicazioni memorizzate sia di effettuare la raccolta in tempo reale dei dati delle comunicazioni degli utenti al di fuori degli Stati Uniti o dei cittadini statunitensi le cui comunicazioni coinvolgevano persone esterne al paese [70].

Cosi nel 2013 Maximilian Schrems avanzò il primo dei due reclami che avrebbero stravolto il mondo del trasferimento dati [71]. Ciò avvenne a seguito delle suddette rivelazioni perché consapevole del rischio di una sorveglianza sociale, estesa e indiscriminata, messa in atto dagli Stati Uniti a seguito del trasferimento dei dati dei cittadini europei.

[69] NSA slides explain the PRISM data-collection program, The Washington Post, 2013, disponibile in: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.
[70] G. Greenwald - E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 2013. Disponibile int: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.
[71] Sentenza della Corte di Giustizia dell'Unione europea del 6 Ottobre 2015, causa C-362/14, *Data Protection Commissioner v. Maximillian Schrems*

Il primo reclamo, dunque, venne presentato il 25 giugno 2013 presso l'Autorità Garante irlandese chiedendo di far cessare a Facebook Ireland [72] il trasferimento dei dati verso gli Stati Uniti, dal momento che tale paese non forniva una protezione conforme a quanto richiesto dalla direttiva[73]. Il trasferimento dei dati personali verso paesi terzi in quegli anni trovava la sua base giuridica nella Decisione di adeguatezza 520/2000/CE anche conosciuta come *Safe Harbor*. Tuttavia, il Commissario irlandese rigettò il reclamo, sostenendo di non essere competente a pronunciarsi in questione, non volendo interferire con quanto stabilito dalla Commissione Europea mediante la Decisione stessa, la quale legittimava i trasferimenti, ritenendo che gli Stati Uniti offrissero un livello di protezione adeguato[74].

La vicenda proseguì con il ricorso del giovane austriaco presso la *High Court* [75], la quale invece riconobbe un "serio dubbio" sul livello di adeguatezza che avrebbe dovuto esser garantito dal Paese d'oltreoceano; infatti, la facoltà di accedere in modo cosi esteso e indiscriminato da parte delle agenzie di *intelligence* ai dati dei diversi *Services Provider* risultava sproporzionata con gli interessi perseguiti. La *High Court* presentò un rinvio pregiudiziale alla Corte di Giustizia dell'Unione, ove si interrogò sul ruolo effettivo delle autorità di controllo indipendenti per la protezione dei dati personali, chiedendosi se potessero condurre una propria indagine sulla questione o se tali autorità fossero assolutamente impossibilitate all'agire in senso contrario alla Decisione 2000/520.

La Corte di Giustizia Europea con la causa *C-362/Maximilian Schrems v. Data Protection Commissioner* stabilì che l'autorità di controllo potesse esaminare le domande relative alla protezione dei dati personali da parte di un interessato, anche in presenza di una decisione da parte della Commissione, e qualora avesse rilevato un'incompatibilità con i principi del diritto europeo, avrebbe potuto promuovere un rinvio pregiudiziale attraverso i giudici della sua nazione [76]. Dall'altra parte, ribadì come la Corte di Giustizia fosse l'unica investita dell'autorità di annullare una decisione di adeguatezza resa dalla Commissione[77].

In quest'occasione oltre ad aver chiarito il ruolo delle autorità indipendenti venne anche annullata la Decisione 520/2000. Infatti la Corte di Lussemburgo, pur riconoscendo l'adeguatezza dei

[72] Maximilian Schrems si rivolse innanzitutto all'Autorità Garante irlandese dal momento che Facebook oltre alla sede legale negli Stati Uniti presenta anche uno stabilimento in Irlanda, da cui trasferiva i dati raccolti in Europa negli Stati Uniti.
[73] Direttiva 95/46/CE all'articolo 25 par. 1 prevedeva 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"
[74] Sentenza della Corte di Giustizia dell'Unione europea del 6 Ottobre 2015, causa C-362/14, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrem*s par. 29.
[75] Corte D'Appello irlandese
[76] Sentenza della Corte di Giustizia dell'Unione europea del 6 Ottobre 2015, causa C-362/14, *Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrem*s, par. 64.
[77] Ivi, par. 52.

principi previsti all'allegato I[78] , che le organizzazioni che si certificavano *Safe Harbor* garantivano di rispettare, sostenne che siffatta decisione permettesse la disapplicazione degli stessi principi per esigenze di sicurezza nazionale senza tuttavia provvedere a delle controgaranzie per gli interessati, rendendo cosi possibile un'ingerenza da parte delle autorità di *intelligence* massiva[79]. Tale accesso generalizzato ai dati degli individui andava senz'altro a ledere il diritto alla protezione dei dati e la tutela della vita privata sanciti agli artt. 7 e 8 della Carta di Nizza, risultando pertanto inammissibile.[80]

Alla luce dell'art. 7 della Carta, ove si afferma il diritto al rispetto della vita privata e della vita familiare, viene riconosciuto che ogni individuo, ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni.[81]

Complementare all'articolo 7 è l'art. 8 della Carta, il quale afferma il diritto alla protezione dei dati personali e precisamente che ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. Inoltre, afferma che i dati personali devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o ad un altro fondamento legittimo previsto dalla legge e che ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica e che il rispetto di tali regole sia soggetto al controllo di un'autorità indipendente.[82]

È bene rammentare come il diritto alla protezione dei dati personali, secondo la concezione europea, non implichi solo la *libertà negativa* di non subire interferenze nella propria vita privata, al cuore del diritto alla riservatezza, ma debba esser inteso anche come *la libertà positiva* di esercitare un controllo sul flusso delle proprie informazioni [83]. Per tale ragione, è pacifico che il diritto alla protezione dei dati personali, concepito come diritto all'autodeterminazione informativa, si traduca con il fatto che l'interessato deve poter prendere una decisione consapevole sulle informazioni che lo riguardano e poter rettificare o cancellare i propri dati se ritiene che tali informazioni non siano più necessarie o siano lesive della sua persona[84]. Tale logica di fondo condusse la Corte a ritenere che

[78] Ivi, par. 79.
[79] Ivi, par. 86.
[80] Guarda P. - Bincoletto, *op cit.,* 137
[81] Carta dei Diritti Fondamentali dell'Unione Europea 2000/C 364/01 art. 7 Rispetto della vita privata e della vita familiare: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni"
[82] Carta dei Diritti Fondamentali dell'Unione Europea 2000/C 364/01 art 8 Protezione dei dati di carattere personale: "1. Ogni 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."
[83] G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, 2017, p.6.
[84] G. Finocchiaro, *la giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in il diritto dell'informazione e dell'informatica,2015, disponibile in: http://romatrepress.uniroma3.it/wpcontent/uploads/2019/05/5lagi-gifi.pdf, 118-119

non fosse conforme al diritto citato una normativa che non solo autorizzasse in maniera generale la conservazione e raccolta di tutti i dati personali degli interessati, trasferiti dall'Unione verso gli Stati Uniti senza alcuna distinzione, limitazione o eccezione a seconda dell'obiettivo perseguito, ma anche non fornisse alcuna tutela giurisdizionale in osservanza dell'articolo 47 della Carta di Nizza. Analogamente, la normativa statunitense non prevedeva alcuna possibilità per il singolo di avvalersi di rimedi giuridici nei confronti delle autorità di intelligence al fine di accedere a dati personali che lo riguardavano, oppure di ottenere la rettifica o la soppressione di tali dati; non rispettando il contenuto essenziale del diritto fondamentale ad una tutela giurisdizionale effettiva.

2.1.1 Dal *Safe Harbor Agreement* al *Privacy Shield*

La Decisione 520/2000 venne cosi annullata dalla Corte nel 2015. Nel frattempo Facebook a seguito dell'annullamento della decisione di adeguatezza aveva già modificato la base giuridica per il trasferimento dei dati scegliendo la sottoscrizione di *standard contractual clauses* [85] in luogo all'adesione a meccanismi di autocertificazione come quelli forniti dalla suddetta decisione.

Il sig. Schrems ripresentò denuncia, sostenendo che ancora gli Stati Uniti non offrissero una protezione sufficiente per giustificare il trasferimento dei dati da parte di Facebook. Chiese di sospendere o vietare, per il futuro, i trasferimenti dei suoi dati personali dall'Unione verso gli Stati Uniti; trasferimenti che, nello specifico, Facebook Ireland effettuava oramai sulla base delle *standard contractual clauses* contenute nell'allegato della decisione 2010/87[7].

Pertanto la denuncia del sig. Schrems questa volta andò ad indagare, in particolare, la validità della Decisione 2010/87. L'Autorità Garante irlandese, sollecitata dallo stesso, avviò un procedimento dinanzi alla *High Court* affinché quest'ultima presentasse alla Corte di Lussemburgo una domanda di pronuncia pregiudiziale. Parallelamente all'avvio di detto procedimento la Commissione adottò la Decisione 2016/1250 sull'adeguatezza della protezione offerta, nota come *Privacy Shield*; adottata a seguito di una dichiarazione di impegni da parte del governo statunitense a creare un meccanismo di vigilanza, il c.d. Mediatore dello scudo [86], sulle ingerenze delle autorità di *intelligence* per motivi di sicurezza nazionale che vengono perpetrate attraverso gli strumenti giuridici

[85] Le *standard contractual clauses* sono state introdotte dalla Commissione nel 2010 a seguito della decisione 2010/87/UE. Esse consentono il trasferimento di dati sulla base di specifiche condizioni da sottoscrivere tra il titolare e il destinatario adottate sullo schema di quelle indicate dalla Commissione.

[86] Il "Mediatore dello scudo", autorità di vigilanza indipendente dotata di poteri di indagine. Secondo quanto stabilito nel Privacy Shield, gli interessati (cittadini di un Paese membro dell'Unione Europea) qualora avessero ritenuto che vi fosse stata un'ingerenza delle autorità di intelligence nei diritti fondamentali della propria persona potevano ricorrere al proprio garante nazionale, al quale poi sarebbe spettato il compito di inoltrare la richiesta al Mediatore dello Scudo. *Caso Schrems II e i trasferimenti di dati personali verso gli Stati Uniti,* Strali, 2020, disponibile in: https://www.strali.org/post/caso-schrems-ii-e-i-trasferimenti-di-dati-personali-verso-gli-stati-uniti.

dell'*Executive Order 12333* [87] del Presidente degli Stati Uniti e l'art. 702 del FISA, in modo tale da tentare di osservare, questa volta, il diritto ad una tutela giurisdizionale secondo quanto sancito all'articolo 47 della Carta di Nizza.

In un primo momento Facebook tentò di sollevare eccezione sostenendo che la domanda pregiudiziale fosse irricevibile, sulla base dell'applicabilità del Regolamento 2016/679 [88] a trasferimenti di dati personali fondati su clausole tipo di protezione contenute nella decisione 2010/87 le quali trovavano la loro base nella direttiva 95/46/CE che era stata abrogata dal Regolamento stesso ai sensi dell'articolo 94) paragrafo 1). La Corte rispose che non solo la direttiva 95/46 era stata abrogata con effetto dal 25 maggio 2018 e pertanto risultava essere ancora in vigore al momento della formulazione della presente domanda di pronuncia pregiudiziale giunta alla Corte il 9 maggio 2018, ma anche che il Regolamento riprendeva sostanzialmente il contenuto della direttiva. Alla base di tali considerazioni la domanda venne ritenuta ricevibile e le questioni avanzate vennero interpretate alla luce del nuovo Regolamento. Per cui la *High Court* in questa occasione sollevò la questione della validità tanto della decisione 2010/87 quanto della decisione 2016/1250 [89].

2.1. La sentenza Schrems II: l'annullamento del *Privacy Shield* e l'incerta condizione delle *standard contractual clauses*

La *High Court* irlandese interrogò la Corte di Giustizia Europea su 11 questioni che possono esser riassunte in questo modo:

Con la prima questione la Corte di Giustizia si interrogò se il Regolamento fosse applicabile a un trasferimento di dati personali effettuato da un operatore economico situato in uno Stato membro verso un altro stabilito in un paese terzo, nel caso in cui tali dati fossero trattati successivamente dalle autorità del suddetto paese, extra UE, per finalità di pubblica sicurezza, difesa e sicurezza dello Stato[90]. Nel caso di specie se l'autorità di *intelligence*, sulla base di strumenti interni quali l'art. *702 del FISA* e *l'Executive Order 12333*, fosse autorizzata a chiedere l'accesso ai dati di Facebook per finalità di sicurezza nazionale. In risposta la Corte affermò che la possibilità che i dati personali fossero trattati per questi fini da parte delle autorità del paese terzo non escludeva il trattamento principale dall'ambito di applicazione territoriale e materiale del Regolamento ai sensi dell'articolo 2) par 1) del Regolamento, non essendo dunque ammissibile far rientrare tal trattamento, attuato a fini commerciali, nei casi di non applicabilità del GDPR ai sensi dell'articolo 2) paragrafo 2).

[87] È un provvedimento emesso dal Presidente deli Stati Uniti che permette la raccolta indiscriminata di informazioni dai provider.
[88] Il Regolamento 2016/679 è entrato in vigore dal 24 maggio 2016
[89] 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*
[90] Ibidem, par. 80.

In merito alle questioni seconda, terza e sesta, l'obiettivo era definire quale dovesse esser il livello di protezione richiesto dall'articolo 46 del Regolamento in merito alle *standard contractual clauses,* chiarendo quali elementi dovessero esser presi in considerazione per determinare se il livello di protezione fosse concretamente garantito nel contesto di un trasferimento di dati personali [91]. Questo si rivelò un passaggio fondamentale nella sentenza, dal momento che, a seguito dell'annullamento della Decisione di adeguatezza 502/2000, c.d. *Safe Harbor*, come detto in precedenza, lo strumento legale che giustificava il trasferimento dei dati adoperato da Facebook erano proprio le *standard contractual clauses*. Sul punto, la Corte di Lussemburgo rispose che il paese terzo non dovesse prevedere un livello di protezione identico, ma "*sostanzialmente equivalente*[92]" a quello europeo secondo quanto stabilito dal Regolamento al considerando 104. In presenza di un trasferimento basato su *standard contractual clauses,* la valutazione di adeguatezza doveva tener conto sia del contenuto delle clausole pattuite tra il titolare del trattamento o il responsabile del trattamento stabiliti nell'Unione e il destinatario del trasferimento stabilito nel paese terzo, sia degli elementi rilevanti del sistema giuridico di destinazione; essi consistono negli stessi elementi che la Commissione deve valutare quando procede all'elaborazione di una decisione di adeguatezza [93]. La Corte in questa occasione ribadì che l'interpretazione del diritto dell'Unione dovesse essere effettuata alla luce di diritti fondamentali garantiti dalla Carta dei diritti fondamentali, sottolineando nuovamente l'importanza degli artt. 7 e 8 della Carta. Pertanto ai sensi dell'articolo 46) paragrafo 1) di detto Regolamento, il titolare del trattamento o il responsabile del trattamento poteva trasferire dati personali verso un paese terzo solo se avesse previsto "*garanzie adeguate"* e a condizione che gli interessati disponessero di *"diritti azionabili e mezzi di ricorso effettivi* [94]".

L'ottava questione, invece, verteva sulla possibilità per un'autorità di controllo di sospendere o vietare un trasferimento di dati personali verso un paese terzo effettuato sulla base delle suddette clausole adottate dalla Commissione, nel caso in cui l'autorità avesse ritenuto che tali garanzie non avessero potuto esser rispettate nel paese destinatario[95]. La Corte rispose in maniera affermativa, sostenendo che se l'autorità al termine della sua indagine avesse ritenuto che l'interessato, i cui dati personali fossero stati trasferiti verso un paese terzo, non avesse goduto in quest'ultimo di un livello di protezione adeguato, sarebbe stata tenuta ad intraprendere misure idonee al fine di porre rimedio all'inadeguatezza constatata.[96]. *Ergo*, l'autorità di controllo venne legittimata a sospendere o a

[91] Ivi, par. 90.
[92] Ivi, par. 91 ss.
[93] Regolamento UE n. 2016/679 articolo 45. par 2.
[94] 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*, par. 103.
[95] Ivi, par. 106.
[96] Ivi, par. 111.

vietare il trasferimento di dati verso un paese terzo effettuato sulla base di *standard contractual clauses* adottate dalla Commissione, qualora avesse accertato che le suddette clausole non fossero o non potessero essere rispettate in tale paese terzo.[97]

Le questioni numero sette e undici invece vertevano sulla validità della Decisione 2010/87/UE relativa alle *standard contractual clauses*, dal momento che l'utilizzo di questo strumento non vincolava le autorità del paese terzo, ma solo le parti che le avevano sottoscritte. La Corte non rilevò nessun elemento per inficiare la validità di tale decisione: in ogni caso il titolare del trattamento e il soggetto destinatario dovevano di volta in volta verificare il livello di protezione garantito nel paese terzo prescelto per non incorrere in una violazione della normativa [98]. Tuttavia, sebbene tali clausole fossero vincolanti per il titolare del trattamento stabilito nell'Unione e per il destinatario del trasferimento di dati personali stabilito in un paese terzo, è pacifico ritenere che esse non potessero vincolare le autorità del paese terzo, poiché queste ultime non erano parti del contratto. Vale a dire che le *standard contractual clauses* che obbligavano le parti contrattuali ad assicurare date garanzie in caso di trasferimento dati non impegnavano le autorità del paese destinatario a rispettare tali garanzie [99].

Infine in merito alla quarta, quinta, nona e decima questione, è stato richiesto alla Corte di valutare la validità della decisione di adeguatezza comunemente nota come *Privacy Shield* con riguardo alle deroghe ai principi garantiti per esigenze di sicurezza nazionale, interesse pubblico o amministrazione della giustizia, e il Mediatore dello scudo[100]. La Corte ha stabilito che la comunicazione di dati personali a un terzo, quale autorità pubblica, costituisse una forma di ingerenza nei diritti fondamentali alla protezione della vita privata e familiare ai sensi dell'art. 7 a e alla protezione dei dati ai sensi dell'art. 8 della Carta. Tali diritti non sono assoluti, possono essere bilanciati con altri, tuttavia, da un'analisi dell'art. 702 del FISA, emerse che il diritto statunitense non prevedesse alcuna limitazione all'autorizzazione per l'attuazione della sorveglianza, né garanzie per i cittadini stranieri potenzialmente soggetti a tali programmi. Questa norma, secondo la Corte, non era idonea a garantire un livello di tutela sostanzialmente equivalente[101]. Nemmeno *l'Executive Order 12333* era idoneo perché non comprendeva un controllo giudiziario all'accesso ai dati, una limitazione alla quantità di informazioni strettamente necessarie alla finalità, alcuna possibilità per il singolo interessato di avvalersi di rimedi giuridici, come un ricorso. Il sistema di sorveglianza, pertanto, risultava sproporzionato. Per quanto riguarda la figura di nuova creazione il c.d. Mediatore dello scudo, era designato dal Segretario di Stato e ciò pose un dubbio sulla sua indipendenza rispetto

[97] Ivi, par. 121 ss.
[98] Ivi, par. 125.
[99] Ivi, par. 125.
[100] Ivi, par. 150 ss.
[101] Ivi, par. 181.

al potere esecutivo, tanto più che non era prevista una possibilità per sanzionare le autorità di *intelligence* non adempienti alle sue decisioni. [102]Alla luce di tali argomentazioni la Corte invalidò la Decisione 2016/1250, c.d. *Privacy Shield*, in quanto contraria ai requisiti previsti dall'art. 45 GDPR e degli artt. 7 e 8 della Carta di Nizza.

2.2.1. Le conseguenze e gli sviluppi dell'annullamento della decisione di adeguatezza 2016/1250: *dall'Executive Order 14086* all'accordo *EU-US Data Privacy Framework*

A seguito dell'annullamento della decisione di adeguatezza 2016/1250 risultante dalla Sentenza C-311/18 comunemente nota come Schrems II, rimasero valide come dichiarato dalla Corte le *SCC,* le quali nel giugno del 2021 vennero aggiornate attraverso la decisione 2021/914/UE. Tuttavia, rispetto ad una decisione di adeguatezza, l'impiego delle *standard contractual clauses*[103]risultava più complesso dal momento che spettava all'esportatore e all'importatore dei dati verificare il rispetto, nel paese terzo, del livello di protezione richiesto dal diritto dell'Unione, ossia se le garanzie previste dalle *standard contractual clauses* potessero essere effettivamente osservate nella pratica[104]. Guardando agli sviluppi in materia di trasferimento dati successivamente alla sentenza Schrems II, la nuova clausola 14 richiedeva alle parti di valutare, prima di concludere gli accordi contrattuali, se le leggi e le prassi del paese terzo di destinazione applicabili al trattamento dei dati personali potessero impedire all'importatore di rispettare le Clausole. Tale verifica dava luogo ad una situazione dubbia, dal momento che l'impiego di queste clausole non poteva vincolare terzi, e nel caso specifico vincolare l'autorità di *intelligence* a rispettarle. Tuttavia un accesso indiscriminato da parte delle autorità pubbliche nei dati degli interessati costituiva un motivo di illegittimità perché metteva l'importatore nelle condizioni di non rispettare le garanzie previste dall'Unione all'interno dell'accordo contrattuale con l'esportatore. Dunque, non garantendo un livello di tutela sostanzialmente equivalente, il trasferimento dati rischiava di divenire oggetto di impugnazione.

Considerate queste premesse, è risultato fondamentale trovare un punto di convergenza affinché tale trasferimento potesse avvenire in maniera sicura e continua, conciliando sia le ragioni dell'economia che vedono lo scambio dei dati come un elemento cardinale per l'economia

[102] Ivi, par. 163 ss.
[103]Ad oggi le *standard contractual clauses* utilizzate anche da Facebook sono quelle allegate nella decisione 2021/914/UE. Queste nuove clausole vanno a sostituire quelle precedenti allegate nella decisione 2010/87/UE le quali non possono più esser utilizzate. M. R. Carbone, *Clausole contrattuali standard per il trasferimento dati: tutto quello che c'è da sapere*,' Cyber Security 360, 2022, disponibile in: https://www.cybersecurity360.it/legal/privacy-dati-personali/clausole-contrattuali-standard-per-il-trasferimento-dati-tutto-quello-che-ce-da-sapere/.
[104] Decisione di esecuzione (UE) 2021/914 della Commissione 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, clausola 14

contemporanea sia le ragioni giuridiche che pongono i diritti dell'interessato al primo posto. Cosi nell'Ottobre del 2022, il Presidente degli Stati Uniti Biden ha firmato *l'Executive Order 14086* "*Enhancing Safeguards for United States Signals Intelligence Activities*" per implementare nella legislazione statunitense quanto stabilito dalla Corte di Giustizia Europea con le sentenze Schrems I e II sulla necessaria limitazione all'accesso ai dati personali da parte dei servizi di *intelligence.* L'*Executive Order*, mira a limitare l'accesso a quanto necessario e proporzionato per proteggere la sicurezza nazionale e istituire un meccanismo di ricorso indipendente e imparziale per gli interessati, dal momento che, come visto precedentemente, l'istituzione di un Mediatore dello scudo non garantiva un giudizio di imparzialità sufficiente [105].

In tale ordine esecutivo sono stati previsti degli ulteriori obblighi in capo alle agenzie di *intelligence* degli Stati Uniti. Ricordando che l'accesso massivo e generalizzato fu una delle ragioni principali che determinarono l'annullamento delle precedenti decisioni di adeguatezza, questa volta gli Stati Uniti mediante questo provvedimento hanno agito sulla libertà di azione dell'intelligence prevedendo che tali attività *(i) siano condotte solo nel perseguimento di obiettivi definiti di sicurezza nazionale; (ii) tengano conto della privacy e delle libertà civili di tutte le persone, a prescindere dalla nazionalità o dal Paese di residenza; (iii) siano condotte solo quando necessario per portare avanti una accertata priorità di intelligence e solo nella misura e con modalità proporzionate a tale priorità*[106].

Un ulteriore elemento cardinale è stata la creazione di un meccanismo di ricorso indipendente su due livelli. Nel primo livello, il funzionario per la protezione delle libertà civili presso l'Ufficio del direttore dell'*intelligence* nazionale, *Civil Liberties Protection Officer*, condurrà una prima indagine sui reclami ricevuti dai cittadini europei per verificare una possibile violazione della normativa (compreso l'ordine esecutivo stesso). Tale provvedimento ha previsto che la decisione del Funzionario sarà vincolante per le agenzie. A garanzia dell'indipendenza delle indagini e delle decisioni del CLPO, come secondo livello di revisione sarà istituito un Tribunale di revisione sulla gestione dei dati personali (DPRC). Il Tribunale avrà lo scopo di fornire un'analisi indipendente e vincolante delle decisioni del Funzionario, su richiesta dell'interessato coinvolto nel caso in cui decidesse di far ricorso alla sua decisione. In ottemperanza all'art 47 della Carta di Nizza, i giudici di questo particolare Tribunale, designati al di fuori del governo degli Stati Uniti, esamineranno i casi in modo indipendente e godranno di una protezione contro la loro rimozione, in modo tale che possa esser garantita un'effettiva tutela giurisdizionale agli interessati.[107]

[105] Guarda P. - Bincoletto, *op cit.,* 138
[106] *Biden firma l'ordine esecutivo per il nuovo privacy Shield*, LegalBlink, 2022, disponibile in https://legalblink.it/post/biden-firma-ordine-esecutivo-privacy-shield.html.
[107] Ibidem

Grazie a tali garanzie, il 10 luglio 2023 la Commissione Europea, dopo 3 anni di intensa negoziazione, ha adottato una nuova decisione di adeguatezza tesa a dichiarare il livello di protezione degli Stati Uniti equivalente a quello dell'Unione Europea. Questa decisione rappresenta un passo significativo nell'ambito di trasferimenti di dati transatlantici, nonché nel contesto del progresso tecnologico e dello sviluppo del commercio tra le due superpotenze. La decisione è progettata per agevolare il flusso transatlantico dei dati in un'epoca in cui le aziende piattaforma giocano un ruolo pervasivo nella vita quotidiana. Tale quadro, inoltre, testimonia un progressivo avvicinamento tra i due modelli, promuovendo una maggiore coerenza e collaborazione in materia di protezione dei dati tra l'Unione Europea e gli Stati Uniti.

CAPITOLO III

IL NUOVO ACCORDO EU - USA TRANSATLANTIC DATA PRIVACY FRAMEWORK

3. La Decisione (UE) 2023/1795: gli aspetti principali della nuova disciplina

Il 10 luglio 2023 scorso è stata adottata dalla Commissione Europea la decisione di adeguatezza finalizzata ad agevolare il flusso transatlantico dei dati. Entrando nel merito della decisione e analizzandone la struttura generale si può notare come la stessa riproduca la medesima struttura delle decisioni di adeguatezza precedenti, *Safe Harbour* e *Privacy Shield*. Analogamente prevede un sistema di certificazione cui i responsabili - titolari del trattamento possono auto-certificare la loro conformità ai principi stabiliti, al fine di ottenere l'autorizzazione a ricevere e gestire i dati provenienti dall'Unione Europea. Tuttavia, una prima differenza emerge nei principi di certificazione, che, rispetto a quelli statuiti nella precedente, *Privacy Shield*, sono stati oggetto di emendamenti finalizzati ad un progressivo allineamento con quanto presente nel Regolamento Generale sulla Protezione dei Dati (GDPR). Il controllo di conformità alla certificazione, ossia del rispetto di questi principi, è stato affidato al *Department of Commerce*[108], mentre le organizzazioni, per essere ritenute eleggibili per la certificazione, devono essere soggette alla giurisdizione della FTC o del DOT, pertanto non tutte possono accedervi[109].

Le organizzazioni che su base volontaria si autocertificano, si impegnano a rispettare alcuni principi e obblighi cardinali nel diritto dell'Unione in materia di protezione dati personali, i quali sono contenuti nell'Allegato I. Interessante osservare come all'interno dell'Allegato in questione vengano adottate definizioni in stile europeo quali ad esempio[110]: dato personale " *dati relativi a una persona fisica identificata o identificabile che rientrano nell'ambito di applicazione del GDPR ricevuti da un'organizzazione negli Stati Uniti dall'UE e registrati in qualsiasi forma*[111]". Il trattamento invece consiste in "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, come la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione o la diffusione, la cancellazione o la distruzione*[112]".

[108] Il *Department of Commerce* è un dipartimento federale del Governo degli Stati Uniti responsabile dello sviluppo economico e delle pratiche commerciali. Si evidenzia come ancora una volta l'impronta fondamentale che distingue il soggetto di tutela emerga anche in questo caso, l'interessato statunitense ossia il consumer trova la sua tutela in tale dipartimento.
[109] Decisione di esecuzione (UE) 2023/1795, par 9 ss.
[110] Ivi, par 11 ss.
[111] Regolamento (UE) n. 2016/679 art. 49) par 1) punto 1).
[112] Regolamento (UE) n. 2016/679 art. 49) par 1) punto 2).

Allo stesso modo, i principi cui le organizzazioni statunitensi devono conformarsi e impegnarsi a rispettare, enucleati all'Allegato 1, sono familiari per chi abita il contesto europeo essendo annoverati tra questi: (i) il principio di limitazione delle finalità, (ii) *accountability*, (iii) trasparenza, (iv) integrità e (v) minimizzazione[113]. Alla luce di quanto detto nel corso dell'elaborato, è risultato di primaria importanza per i cittadini europei l'introduzione di diritti individuali, primo tra tutti quello di accesso ai dati. Ciò si è rivelato decisivo per la Commissione nel momento in cui la decisione è stata adottata, perché nella concezione europea la presenza di tali diritti è manifestazione della *libertà positiva* dell'individuo di controllare le proprie informazioni, in ossequio al diritto di autodeterminazione informativa, concetto enucleato agli artt. 7 e 8 della Carta di Nizza. Allo stesso modo il *data subject* ha diritto ad ottenere la rettifica dei dati corretti in linea con il principio di integrità dei dati[114]. Altro principio cui devono aderire gli organismi che si certificano è senz'altro quello di *accountability* [115] , secondo il quale i soggetti che trattano i dati sono tenuti a predisporre misure tecniche e organizzative adeguate ad adempiere efficacemente ai loro obblighi di protezione dei dati e a essere in grado di dimostrare tale conformità all'autorità di controllo competente.

Pertanto una volta che un'organizzazione ha deciso volontariamente di certificarsi [116] ai sensi del DPF UE-USA, la sua effettiva conformità ai principi è obbligatoria. Di conseguenza, le organizzazioni, in ossequio al principio di *accountability*, devono preoccuparsi di adottare misure opportune per verificare che le loro politiche sulla privacy siano conformi ai principi e che vengano effettivamente rispettate[117] . Ciò può avvenire sia attraverso un sistema di autovalutazione, che deve includere procedure interne finalizzate ad una formazione del personale sul come attuare le politiche privacy dell'organizzazione stessa, sia attraverso verifiche esterne della conformità, i cui metodi possono includere audit, controlli casuali o l'uso di strumenti tecnologici.

Le organizzazioni devono conservare la documentazione relativa all'attuazione delle loro pratiche DPF UE-USA e renderla disponibile su richiesta nell'ambito di un'indagine o di un reclamo di non conformità all'autorità giurisdizionale competente. Il DPF UE-USA sarà amministrato e monitorato dal Ministero della Difesa, tuttavia il controllo della certificazione degli organismi spetterà, come detto, al DOC, esonerando l'imprenditore dal laborioso percorso di verifica di conformità.

Inoltre il DPF sarà sottoposto periodicamente ad una revisione. La prima sarà ad un anno dall'adozione della decisione, sia da parte della Commissione Europea che da parte delle Autorità

[113] Decisione di esecuzione (UE) 2023/1795, par 13 ss.
[114] Ivi, par 30
[115] Ivi, par 44
[116] Ivi, par 63
[117] Ivi, par 65

Garanti Europee. Per quanto concerne l'attività di *compliance*, l'impegno a rispettare i principi del DPF dovrà risultare chiaramente nelle informative sulla privacy delle organizzazioni statunitensi. L'imprenditore italiano, allo stesso modo, dovrà aggiornare le informative, indicando espressamente l'utilizzo di organizzazioni che aderiscono al DPF. Inoltre, gli interessati al trattamento dei dati personali potranno rivolgersi direttamente al soggetto statunitense per ricevere informazioni in relazione ai dati personali trattati e ai diritti esercitabili ai sensi degli articoli 15 e seguenti del GDPR. L'esercizio di tali diritti è una prerogativa fondamentale per poter ottenere l'autocertificazione.

3.1.1. Il DOC: l'amministrazione centrale del DPF

Il DPF UE - USA sarà supervisionato dal Dipartimento del Commercio degli Stati Uniti, responsabile dell'elaborazione delle richieste di certificazione e del controllo sulle imprese partecipanti, assicurandosi che continuino a soddisfare i requisiti di certificazione. Inoltre tali organizzazioni saranno obbligate a procedere con una ri-certificazione su base annuale e saranno tenute a dichiarare il loro impegno ad osservare i Principi, a rendere disponibili le loro politiche sulla privacy e ad attuarle[118]. Nell'ambito della richiesta di certificazione, le organizzazioni devono presentare al DOC le informazioni concernenti: il nome dell'organizzazione in questione, una descrizione delle finalità per le quali l'organizzazione tratterà i dati personali, i dati personali che saranno coperti dalla certificazione, nonché il metodo di verifica prescelto, il meccanismo di ricorso indipendente pertinente e l'organismo statutario che ha giurisdizione nel far rispettare i Principi. Qualsiasi falsa dichiarazione al pubblico da parte di un'organizzazione in merito alla sua adesione ai Principi è soggetta ad azioni di applicazione da parte *dell'FTC, del DoT*.

Per garantire la corretta applicazione del DPF UE - USA, le parti interessate: i *data subject*, gli esportatori e le autorità nazionali per la protezione dei dati, devono essere in grado di identificare le organizzazioni che aderiscono ai Principi. Per garantire tale trasparenza, il DOC si è impegnato per rendere disponibile al pubblico l'elenco delle organizzazioni che hanno certificato la loro adesione ai Principi. Il Ministero della Difesa invece è incaricato di aggiornare l'elenco sulla base della presentazione annuale di una nuova certificazione da parte di un'organizzazione e ogni volta che un'organizzazione si ritira o viene rimossa dal DPF UE-USA[119].

[118] Ivi, par 67
[119] Ivi, par 52

3.2. Il ruolo di indagine nei confronti degli operatori economici certificati: la FTC la tutela degli interessati.

Uno dei profili senz'altro più interessanti, in linea con la presente trattazione, riguarda il ruolo della FTC all'interno di questo quadro. Infatti al fine di garantire un livello adeguato di protezione dei dati nella pratica, è necessaria la presenza di un'autorità di vigilanza indipendente dotata di poteri di controllo e di applicazione delle norme di protezione dei dati, conformemente con quanto statuito all'articolo 51 del GDPR. Pertanto le organizzazioni che si certificano DPF UE-USA devono essere soggette alla giurisdizione delle autorità statunitensi competenti - *la FTC e il DoT* – le quali hanno i necessari poteri di indagine e di applicazione per garantire effettivamente il rispetto dei principi[120]. L'FTC dispone di ampi poteri di applicazione nella sfera civile al fine di promuovere la tutela dei consumatori per tali ragioni può applicare a una vasta gamma di leggi finalizzate alla tutela della vita privata e alla sicurezza dei consumatori e dei dati che li riguardano [121].

Eventuali violazioni di tali principi sono perseguibili ai sensi della Sezione 5 dell'FTC Act che vieta atti sleali e ingannevoli nel commercio. Come visto precedentemente la FTC si impegna affinché venga sventato il rischio di una sorveglianza commerciale; all'Allegato 4 si dichiara che i consumatori europei avranno diritto alle medesime tutele previste per i *consumers* statunitensi. Guardando ai precedenti sono diverse le occasioni in cui la FTC è intervenuta a sanzionare operatori statunitensi poiché le loro condotte sono state ritenute illecite e dannose anche per i consumatori europei. Ad esempio nel caso FLO [122] , applicazione finalizzata al monitoraggio della fertilità, la FTC intervenne quando la nota applicazione fu accusata di divulgare dati con parti terze di analisi, dopo essersi impegnata a mantenere private tali informazioni. Pertanto per tale trattamento, effettuato senza alcuna base giuridica, non rispettando i principi presenti nell'allora vigente *Privacy Shield,* venne disposto un ordine da parte della FTC nei confronti dell'applicazione ad inibire la propria condotta, a notificare agli interessati la divulgazione e invitare le parti terze, cui i dati erano stati divulgati, a distruggerli. Aspetto che funge da riprova del fatto che gli ordini della FTC proteggono tutti i consumatori di tutto il mondo che interagiscono con un'azienda statunitense, non solo quelli che hanno presentato reclami.

Una volta ricevuta la segnalazione da parte del Dipartimento del Commercio, dalla DPA di uno Stato membro dell'UE, la FTC può intraprendere una serie di azioni per affrontare le questioni sollevate. Ad esempio, può esaminare le politiche sulla privacy dell'organizzazione, ottenere ulteriori

[120] Ivi, par 59
[121] Allegato IV par 1) punto a), Decisione di esecuzione (UE) 2023/1795
[122] *FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others*, 2021, disponibile in: https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

informazioni direttamente dall'organizzazione o da terzi. La FTC può indagare sull'osservanza dei Principi e sulle false dichiarazioni di adesione ai Principi o di partecipazione al DPF UE-USA, anche in maniera autonoma senza la segnalazione. Inoltre può imporre l'osservanza delle norme richiedendo ordini amministrativi o di tribunali federali e monitorare sistematicamente l'osservanza di tali ordini. Se le organizzazioni non si conformano a tali ordini, la FTC può chiedere sanzioni civili e altri rimedi, anche per eventuali danni causati dalla condotta illecita. Altro aspetto importante guarda la collaborazione fra la FTC e l'EDPB, infatti L'FTC si impegnerà a condurre regolari incontri con i rappresentanti designati del Comitato Europeo per la Protezione dei Dati (EDPB) per esaminare e promuovere ulteriori miglioramenti nella cooperazione operativa in generale. Inoltre, parteciperà attivamente, in collaborazione con il Dipartimento del Commercio, la Commissione Europea e i rappresentanti dell'EDPB, alla periodica valutazione dell'attuazione del Data Privacy Framework UE-USA per discutere le relative implementazioni.

3.2.1 I meccanismi di ricorso per gli interessati in caso di mancata conformità dell'organismo ai Principi

Per garantire una protezione adeguata e, in particolare, l'applicazione dei diritti individuali, l'interessato deve disporre di un ricorso amministrativo e giudiziario efficace [123]. Il DPF UE-USA, attraverso il principio del *ricorso, dell'applicazione e della responsabilità*[124], richiede alle organizzazioni di prevedere un ricorso per le persone interessate in caso di mancata conformità che si traduce con la possibilità per gli interessati dell'Unione di presentare reclami in merito alla mancata conformità da parte delle organizzazioni del DPF UE-USA e di ottenere che tali reclami siano risolti, se necessario, con una decisione che fornisca un rimedio efficace. Le organizzazioni certificate hanno l'onere di soddisfare i requisiti di questo principio prevedendo meccanismi di ricorso indipendenti ed efficaci attraverso i quali i reclami e le controversie di ciascun individuo possano essere esaminati e risolti rapidamente senza alcun costo per l'individuo[125].

Le organizzazioni statunitensi hanno la libertà di scegliere i meccanismi di ricorso indipendenti nell'Unione o negli Stati Uniti. Pertanto, gli interessati possono presentare un reclamo direttamente a un'organizzazione o a un organismo indipendente di risoluzione delle controversie designato dall'organizzazione, ad esempio: alla DPA nazionali o alla FTC[126]. Tra le varie possibilità emerge l'intenzione di impegnarsi volontariamente a cooperare con le autorità di protezione dei dati dell'UE. Dunque, il DPF UE-USA offre agli interessati una serie di possibilità per far valere i propri

[123] Decisione di esecuzione (UE) 2023/1795, par 65
[124] Ivi, par 45
[125] Ivi, par 66
[126] Ivi, par 68

diritti, presentare reclami in caso di non conformità da parte delle organizzazioni UE-USA e di ottenere la risoluzione dei loro reclami, se necessario con una decisione che fornisca un rimedio efficace.

Alcune di queste possibilità sono [127]:

1. In primo luogo, gli interessati dell'Unione possono perseguire i casi di non conformità ai principi attraverso contatti diretti con le organizzazioni DPF UE-USA. Per facilitare la risoluzione, l'organizzazione deve mettere in atto un meccanismo di ricorso efficace per gestire tali reclami. La politica sulla privacy di un'organizzazione deve quindi informare chiaramente le persone su un punto di contatto, interno o esterno all'organizzazione, che si occuperà dei reclami
2. In secondo luogo, le persone possono anche presentare un reclamo direttamente all'organismo indipendente di risoluzione delle controversie (negli Stati Uniti o nell'Unione) designato da un'organizzazione per indagare e risolvere i reclami individuali (a meno che non siano palesemente infondati o futili) e per fornire un ricorso appropriato e gratuito alle persone.
3. In terzo luogo, gli interessati possono anche presentare i loro reclami a un'autorità nazionale di protezione dei dati nell'Unione, che può avvalersi dei propri poteri investigativi e correttivi ai sensi del Regolamento 2016/679.

Mentre per quanto riguarda i cittadini americani, la protezione dati al momento è una materia statale disciplinata solo in alcuni stati e non esiste una legge federale uniforme in materia. Un esempio significativo è lo stato della California ove è presente una normativa simile al GDPR, che tuttavia presenta una differenza sostanziale: è diretta a disciplinare la tutela dei *consumers* non delle persone fisiche. I consumatori che abitano lo stato della California per l'esercizio dei diritti garantiti quali ad esempio: *right to be informed, right to access, right to stop to sale,* possono rivolgersi direttamente all'organizzazione la quale deve, al fine di essere *compliant*, predisporre un numero verde per permettere l'esercizio diretto dei diritti. In caso di mancata conformità le aziende che non rispettano la presente normativa possono esser soggette a sanzioni elevate per ciascuna violazione; l'ammontare della violazione può crescere a seconda dell'entità e del numero di individui coinvolti. In aggiunta ai *consumers* è data la possibilità di esperire *class action* in caso di violazione di protezione dei dati personali. Per quanto riguarda la generalità dei consumatori statunitensi in caso di problemi legati alla protezione dei loro dati personali nei confronti di un'organizzazione statunitense non troveranno protezione all'interno del data privacy framework, il quale prevede una tutela per gli *interessati* che abitano il contesto europeo e si rapportano con le organizzazioni statunitensi. Ad oggi negli Usa non vi è ancora una legge federale finalizzata a fornire le necessarie garanzie a protezione dei dati degli

[127] Ivi, par 67 ss.

individui. Tuttavia è importante sottolineare che una forma di tutela dei dati dei consumatori statunitensi è data dalla FTC. Infatti, gli interventi di questa agenzia governativa sono volti a tutelare il consumatore da pratiche commerciali scorrette. Pertanto un utilizzo improprio dei dati personali finalizzato ad indurre il consumatore a determinate azioni a seguito di profilazione con l'obiettivo di profitto, è sanzionato a livello federale perché tale comportamento, sorveglianza commerciale, costituisce una pratica scorretta a danno dei consumatori.

3.3 Il necessario bilanciamento tra sicurezza pubblica e diritti fondamentali degli interessati

Altro punto critico su cui la presente decisione ha cercato di porre rimedio, riguarda l'ingerenza da parte delle autorità di *intelligence*[128]. È stato statuito dall'*Executive Order* 14086 del 7 ottobre 2022 che le autorità di *intelligence* possano accedere ai dati personali per ragioni di pubblica sicurezza, purché tali ingerenze siano necessarie, proporzionate, e avvengano per finalità specifiche. Nell'*Executive Order*, le imprese statunitensi che ricevono dati dall'Unione Europea sono tenute a sospendere l'applicazione dell'accordo quando ciò interferisca con esigenza di pubblica sicurezza, tuttavia, in ossequio al principio di proporzionalità l'*Executive Order* ha limitato tali ingerenze ad una serie di scopi legittimi che possono giustificare le attività di intelligence e presenta un elenco di circostanze in cui tali attività sono invece proibite[129].

Inoltre, per garantire un'effettiva tutela giurisdizionale, nei confronti dell'operato delle agenzie *di intelligence*, è stata prevista l'istituzione del *Data Protection Review Court*, un tribunale indipendente volto ad analizzare l'operato del Funzionario, CLPO, incaricato di verificare se l'intervento delle autorità di intelligence sia stato proporzionato o meno ai sensi della normativa vigente, incluso anche l'*Executive Order* 10486. Come visto precedentemente l'istituzione di questo meccanismo di controllo sull'agire dell'*intelligence* ha come obiettivo quello di bilanciare le ragioni di sicurezza pubblica con la protezione dei diritti fondamentali degli interessati, i quali non solo hanno diritto ad una protezione delle proprie informazioni nei confronti delle autorità di un paese terzo ma anche hanno diritto ad un'effettiva tutela giurisdizionale, che disponga di un effettivo potere sanzionatorio nei confronti di dette autorità. Gli interessati hanno la possibilità di impugnare la decisione del funzionario per la protezione delle libertà civili, CLPO, davanti al tribunale di revisione della protezione dei dati (DPRC). Il tribunale è composto da membri nominati previa consultazione con il Segretario Generale e il Presidente del DOC, i quali sono designati sulla base di specifiche qualifiche e possono essere licenziati solo per motivi tassativi e non dovrebbero ricevere istruzioni

[128] Ivi, par 119

[129] M. Giacalone, *Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework*, European Papers, disponibile in: https://doi.org/10.15166/2499-8249/644, 152-153

dal governo. Il DPRC ha il potere di indagare sui reclami dei cittadini dell'UE e può adottare decisioni vincolanti per rimediare, aspetto che lo contraddistingue dal Mediatore precedente il quale non aveva il potere di adottare decisioni vincolanti, ma svolgeva un ruolo meramente consultivo. Ad esempio, se il DPRC scopre che i dati sono stati raccolti in violazione delle garanzie previste dall'Executive Order, può ordinarne la cancellazione.

3.4 Verso una possibile sentenza Schrems III: le criticità del nuovo regolamento

Nonostante vi siano stati evidenti miglioramenti rispetto la precedente decisione, a riprova del tentativo di avvicinare i due sistemi, anche questa volta vi sono alcune criticità specie in merito all'ingerenza delle autorità pubbliche e all'indipendenza degli organi giurisdizionali preposti alla risoluzione delle controversie, ossia il DPRC. Con riferimento alle interferenze perpetrate dalle autorità pubbliche risulta problematica l'interpretazione data dei principi di necessità e proporzionalità. In particolare, il concetto di accesso "proporzionato" ai dati, definito dalla giurisprudenza statunitense, potrebbe non essere in linea con l'art 52 della Carta di Nizza. Per quanto concerne il principio di proporzionalità, l'*Executive Order* 14086 evidenzia, ancora una volta, il predominio dell'esigenza di sicurezza nazionale in virtù della quale le organizzazioni statunitensi che ricevono dati dall'Unione sono tenute a disapplicare l'accordo qualora questo interferisse con tale esigenza. L'*Executive Order*, come visto, rispetto al precedente, ha definito una serie di obiettivi legittimi che giustificano le attività di intelligence e un elenco di casi in cui invece suddette attività non son ammesse. Tuttavia, in conformità all'art. 52 della Carta, le limitazioni dei diritti fondamentali riconosciuti dalla Carta dei diritti fondamentali dell'Unione possono essere apportate solo ove siano necessarie e mirino a perseguire finalità di interesse generale riconosciute dell'UE o siano volte a proteggere i diritti e le libertà altrui [130]. Proprio riguardo alla conformità di tale provvedimento con l'art 52 sorgono alcune problematiche, innanzitutto: la base giuridica dell'ingerenza nel diritto fondamentale, la quale deve essere chiara, precisa e prevedibile. Nel testo dell'*Executive Order*, gli obiettivi legittimi che giustificano le attività di intelligence hanno una formulazione generica che permette un'interpretazione eccessivamente ampia. Pertanto diviene pacifico dubitare della chiarezza e precisione della limitazione. Altro punto critico concerne il requisito della prevedibilità dell'applicazione della misura poiché nell'Executive Order 14086 è indicato come tali obiettivi possano essere emendati dal Presidente in caso di rischio alla sicurezza nazionale. Un ulteriore problema, invece, è dato dal fatto che tale Executive Order non sarebbe intervenuto sulla normativa concernente la sez. 702 *FISA* e l'*Executive Order 12333*, disposizioni che come visto

[130] Ibidem

precedentemente, erano già state valutate negativamente dalla Corte di giustizia. Tanto che nelle sentenze Schrems la Corte ha concluso che tale normativa non è conforme ai requisiti richiesti dal diritto dell'Unione, in ossequio al principio di proporzionalità; poiché tali normative, che permettono interferenze nei diritti fondamentali, non definiscono la portata della limitazione dei diritti fondamentali ex artt. 7 e 8 della Carta non prevedendo norme ben definite.

I nodi critici in relazione all'operato del DPCR, di recente istituzione, riguardano la valutazione dell'attività svolta del CLPO a seguito del reclamo presentato dall'interessato. Il tribunale è incaricato di valutare la formale correttezza della procedura svolta dal CLPO, tuttavia non è previsto il riconoscimento all'interessato l'esercizio del controllo sui propri dati quando trattati dall'*intelligence*, non rispettando in tal modo il principio dell'autodeterminazione informativa. Infatti, il meccanismo delineato dall'*Executive Order* non conferisce ai ricorrenti il diritto di ottenere l'accesso, la rettifica o la cancellazione dei propri dati personali quando trattati dai servizi di *intelligence*, inoltre non è prevista alcuna possibilità di ottenere il risarcimento dei danni, come invece garantito a livello europeo dall'art. 82 GDPR. Dunque, essendo statuito nel GDPR che anche il trattamento per esigenze di sicurezza nazionale richieda le dovute garanzie e limitazioni, l'impossibilità di accedere ai propri dati sebbene raccolti da autorità per ragioni di pubblica sicurezza, mette legittimamente in dubbio il rispetto da parte del sistema statunitense del requisito di *equivalenza sostanziale* al sistema europeo[131]

[131] Ivi, 154-155

CONCLUSIONI

In chiusura di questa trattazione, con l'auspicio di aver condotto il lettore attraverso un percorso volto a delineare due sistemi di natura differente, che hanno dato corpo a concezioni diverse del dato personale, emergono importanti diverse considerazioni. La preminente esigenza di proteggere l'interesse pubblico, attraverso una giustificata intrusione nei dati personali degli individui, inclusi quelli al di fuori del territorio statunitense, e la necessità di promuovere lo sviluppo economico, specialmente per quanto riguarda le aziende piattaforma, che quasi considerano il dato come merce di scambio, entrano in conflitto con la tutela del dato personale europeo. La protezione dei dati personali, alla luce della combinazione degli articoli 7 e 8 della Carta di Nizza, si traduce nella libertà positiva dell'individuo di esercitare un controllo attivo sulla propria vita e sulle questioni che lo riguardano, riflessa nel principio *dell'habeas data* che in ossequio con il principio di autodeterminazione informativa ha contribuito alla formazione dei diritti dell'interessato sanciti nel GDPR.

Un'analisi sulla a natura dicotomica dei dati personali è poi stata condotta per evidenziarne le potenzialità e, allo stesso tempo, la necessità di tutela. Permettendo di comprendere perché e quanto la proiezione in rete dell'individuo sia meritevole di protezione. L' opinione di chi scrive è che, nell'era digitale e dei dati, il progresso economico richieda un flusso transatlantico che agevoli lo scambio, fondamentale per molti modelli di *business* contemporanei. D'altra parte, è innegabile che le garanzie europee rappresentino un modello da seguire. La recente decisione di adeguatezza dimostra che gli standard degli Stati Uniti possono essere adeguati a garantire uno scambio commerciale sicuro ed efficiente, bilanciando le esigenze economiche con la tutela dell'individuo, la protezione e il controllo dei dati da lui prodotti.

Tuttavia, considerando gli aspetti tecnici delineati dal nuovo quadro, è difficile dichiararsi soddisfatti o affermare di aver raggiunto l'obiettivo di un sistema armonizzato tra le due superpotenze. Gli Stati Uniti non dispongono ancora di una legge federale sulla protezione dei dati, e il loro modello di regolamentazione rimane orientato principalmente verso l'aspetto economico e la sicurezza nazionale. Nonostante i notevoli miglioramenti e l'impegno dichiarato degli Stati Uniti a soddisfare le esigenze degli interessati, sembra che il processo di convergenza in corso tra i due sistemi non sia ancora in grado di soddisfare il requisito di *equivalenza sostanziale* stabilito dalla Corte di Giustizia dell'Unione Europea

BIBLIOGRAFIA

A.Bradford, *The European Union in a globalised world: the Brussels effect*, 2021

A. Soro, *Un'economia basata sui dati*, intervento, 14 Novembre 2019: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/3545472

Biden firma l'ordine esecutivo per il nuovo privacy Shield, LegalBlink, 2022: https://legalblink.it/post/biden-firma-ordine-esecutivo-privacy-shield.html

B.Saetta, *Protezione dati personali: la privacy negli USA*: https://protezionedatipersonali.it/privacy-negli-usa

Carta dei Diritti Fondamentali dell'Unione Europea 2000/C 364/01

C.D'Cunha, *Idee di Giovanni Buttarelli, trascritte da Christian D'Cunha*, in *Privacy 2030. Una nuova visione per l'Europa*, Garante per la protezione dei dati personali, International Association of Privacy Professionals, novembre 2019

C.Duhigg, *How companies learn your secrets*, The New York Times Magazine, 2012: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

Caso Schrems II e i trasferimenti di dati personali verso gli Stati Uniti, Strali, 2020: https://www.strali.org/post/caso-schrems-ii-e-i-trasferimenti-di-dati-personali-verso-gli-stati-uniti

Decisione di esecuzione (UE) 2023/1795

F.Banterle, *Pubblicità comportamentale, GDPR e rischi di discriminazione In: Società delle tecnologie esponenziali e General Data Protection Regulation: Profili critici nella protezione dei dati*. Milano, Ledizioni, 2018: http://books.openedition.org/ledizioni/3943

FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others, 2021: https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google.

Garante per la protezione dati personali, *Facebook, i dati personali possono essere corrispettivo di un servizio? Lecito dubitarne*: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9575591.

G. Finocchiaro, *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Bologna, 2017, p.6.

G. Finocchiaro, *la giurisprudenza della Corte di giustizia in materia di dati personali da Google Spain a Schrems*, in il diritto dell'informazione e dell'informatica, 2015: http://romatrepress.uniroma3.it/wpcontent/uploads/2019/05/5lagi-gifi.pdf

G. Greenwald - E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, The Guardian, 2013.: https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

M. Giacalone, *Verso Schrems III? Analisi del nuovo EU-US Data Privacy Framework*, European Papers: https://doi.org/10.15166/2499-8249/644

M. Minghetti, *l'era delle aziende piattaforma*, Sole 24 ore, 2016: https://marcominghetti.nova100.ilsole24ore.com/2016/07/18/era-delle-aziende-piattaforma/

M.L.G Sakamoto, *International data transfer. An analysis of schrems cases I and II*, In Seven Editora eBooks. 2023

M. R. Carbone, *Clausole contrattuali standard per il trasferimento dati: tutto quello che c'è da sapere*,' Cyber Security 360, 2022: https://www.cybersecurity360.it/legal/privacy-dati-personali/clausole-contrattuali-standard-per-il-trasferimento-dati-tutto-quello-che-ce-da-sapere/

N. Bernardi, *Privacy. Protezione e trattamento dei dati*, 2019

NSA slides explain the PRISM data-collection program, The Washington Post, 2013: https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/

P.Guarda - G. Bincoletto, *Diritto comparato della privacy e dei dati personali*, Ledizioni, 2023

P. Darnis, *Le relazioni transatlantiche al tempo del digitale: la questione del trasferimento di dati*, Istituto Affari Internazionali, 2021

P. M.Schwartz and K. N. Peifer, *Transatlanti Data Privacy Law,* Georgetown law journal, 2017: https://escholarship.org/uc/item/1ws1r1cz

R. Berti - F. Zumerle, *Privacy negli Usa a che punto sono le prime regole nazionali*, 2022: https://www.agendadigitale.eu/sicurezza/privacy/privacy-negli-usa-a-che-punto-sono-le-prime-regole-nazionali/

Regolamento (UE) n. 2016/679

R. Levine, *Behind the European Privacy Ruling That's Confounding Silicon Valley*, N.Y. Times, 2015: https://www.nytimes.com/2015/10/11/business/international/behind-the-european- privacy-ruling-thats-confounding-silicon-valley.html [https://nyti.ms/2py7rQX]

S. Warren, L. D. Brandeis, *The Right to Privacy*, in *Harvard Law Review*, Vol. 4, No. 5, 1890

S. Rodotà, *Il mondo nella rete. Quali i diritti, quali i vincoli*, Laterza, Roma-Bari 2001

S. Rodotà, *la vita e le regole: tra diritto e non diritto*, Feltrinelli, Milano 2006

S. Rodotà, *Privacy Freedom and Dignity: conferenza internazionale sulla protezione dei dati personali*: https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/1049293

S. Rodotà, *Tecnologie e diritti*, Bologna, 1995

Sentenza della Corte di Giustizia dell'Unione europea del 6 Ottobre 2015, causa C-362/14, *Data Protection Commissioner v. Maximillian Schrems*

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*