UNIVERSITÀ DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI "M.FANNO"

DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN ECONOMIA E MANAGEMENT

PROVA FINALE

"STRUMENTI INFORMATICI E TUTELA DEI DATI PERSONALI: DAL SAFE HARBOR AGREEMENT AL PRIVACY SHIELD AGREEMENT"

RELATORE:

CH.MA PROF.SSA CLAUDIA SANDEI

LAUREANDA: VALERIA LOLLO

MATRICOLA N. 1066215

ANNO ACCADEMICO 2015 – 2016

Indice

1. INTRODUZIONE

Attualmente, uno dei temi che assume crescente importanza nel quadro giuridico internazionale si sostanzia nelle dinamiche concernenti la tutela dei dati personali, la privacy e le relazioni che possono essere stabilite tra le imprese sulla base delle informazioni che queste ottengono dai propri utenti attraverso la navigazione sulle piattaforme digitali.

In questo frangente, tanto Unione Europea quanto Stati Uniti si dimostrano consapevoli della delicatezza di tale tematica e appaiono interessati ad assicurare le misure consone alla protezione dei dati al fine di mantenere le loro relazioni stabili sia sotto il profilo economico che sotto il profilo di sicurezza nazionale e tutela dei propri cittadini. Si rende quindi necessario prendere in considerazione il quadro normativo che appare frammentario ed eterogeneo ma che allo stesso tempo si vede protagonista di numerosi interventi legislativi attuati con la finalità di ottenere un sistema di supervisione più organico.

Il seguente elaborato si pone l'obiettivo di analizzare i cambiamenti che hanno interessato lo scenario normativo internazionale alla luce delle rivelazioni sui programmi di intelligence statunitense da parte di Edward Snowden[1] i quali a loro volta hanno messo in atto un meccanismo capace di sovvertire le dinamiche legate alla trasmissione e trasformazione dei dati personali, anche grazie alla causa al social network Facebook promossa da Maximilian Schrems.[2]

Si partirà quindi dall'esaminare i diversi approcci con cui Unione Europea e Stati Uniti si avvicinano alla tematica della tutela dei dati personali. Si cercherà, inoltre, di fornire una panoramica sul principale accordo a cui le due superpotenze sono giunte prima del caso Schrems, il Safe Harbor Agreement.

Infine, verrà affrontato l'attuale accordo in materia entrato in vigore il 12 luglio del 2016, il Privacy Shield Agreement, individuando i punti chiave dello stesso e mettendo in luce le caratteristiche che lo differenziano dal precedente Safe Harbor Agreement.

[1] Edward Snowden è un informatico statunitense e fino al 10 giugno 2013 collaboratore di un'azienda di tecnologia informatica consulente della National Security Agency (NSA). Si è reso noto nello scenario internazionale attraverso la rivelazione di numerosi dettagli inerenti a programmi di sorveglianza di massa dei governi statunitense e britannico, fino a quel momento tenuti segreti.

[2] Maximilian Schrems è un attivista austriaco che si è impegnato nel promuovere una causa contro Facebook Ireland Ltd, concentrandosi sulla violazione di privacy, sulla violazione delle leggi comunitarie in materia di protezione dei dati personali e il trasferimento di informazioni private alla National Security Agency.

2. LE "PLATFIRM": UN NUOVO MODELLO DI IMPRESA E L'UTILIZZO DEI DATI PERSONALI

In connessione ai profondi cambiamenti legati allo sviluppo e alla diffusione degli strumenti informatici e alla trasformazione indotta dai social network, si vede diffondersi a livello globale il fenomeno delle "Platfirm" definite come nuovi modelli di business agevolati dall'estensione della rivoluzione digitale.

L'aspetto caratterizzante delle imprese-piattaforma si sostanzia nella loro struttura: un'architettura costituita di software e hardware con la funzione di aggregatore e organizzatore di risorse, transazioni, relazioni tra individui e diversi attori con la finalità di co-creare valore.[3]

In questa direzione, l'elemento dirompente rispetto all'idea tradizionale di impresa è rappresentato dallo scambio di dati[4] e informazioni personali[5]. Secondo questo nuovo schema infatti, la piattaforma facilita le interazioni e contatti tra produttori e consumatori permettendo di creare valore all'esterno dei confini aziendali e di far beneficiare dello stesso sia coloro i quali sono interessati a finalità di coproduzione sia coloro i quali si avvicinano alla struttura digitale con l'intenzione di godere dei servizi che vengono proposti. Si diffonde in questo modo l'approccio definito "interaction-first", sostitutivo del precedente "user-first" impiegato dall'impresa tradizionale, il quale nasce con lo scopo di massimizzare l'efficienza e la ripetibilità dell'interazione tale da renderla una base solida per la creazione e lo scambio di valore.

Si rende quindi evidente come tra le diverse leve di cui tali imprese possono fare uso per il conseguimento dei propri obiettivi di business assuma un crescente risalto lo scambio di dati. Nello specifico, viene attribuito particolare spessore ai dati e alle informazioni che gli enti, siano essi pubblici o privati, riescono a pervenire dalla navigazione di utenti iscritti a piattaforme digitali e social network. Le dinamiche che configurano lo scenario competitivo attuale e futuro rendono lo scambio e la condivisione di dati un elemento imprescindibile per la gestione imprenditoriale poiché permettono di estrarne un patrimonio di informazioni e collegamenti essenziali per la

[3] Marco Minghetti, luglio 2016, Supplemento allegato al n. 7/8 Luglio-Agosto 2016 di Harvard Business Review, http://marcominghetti.nova100.ilsole24ore.com/2016/07/18/era-delle-aziende-piattaforma/

[4] D.Lgs.30 giugno 2003, n.196, Art. 4 1. b) ""dato personale", qualunque informazione relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale".

[5] Parere 4/2007 (WP 136)- Dato Personale, "[…] In merito al formato, infine, non rileva la tipologia di supporto che contiene l'informazione. Qualsiasi forma (acustica, fotografica, numerica,…) comunque registrata (su carta, in formato elettronico, ecc,…) è rilevante".

gestione della propria attività economica e sono fonte di vantaggio competitivo qualora opportunamente utilizzati.

Sono tre, fondamentalmente, le attività di cui le imprese si occupano nell'ambito della raccolta dei dati:

1. L'acquisizione remota dei dati e la successiva trasmissione ai propri server, funzione che oggigiorno sembra essere estesa in modo pervasivo.
2. La registrazione e la ricerca di dati la quale fa riferimento all'utilizzo di database che tengano traccia dei diversi stati che le informazioni assumo dal momento in cui vengono raccolte a quando successivamente sono processate e utilizzate.
3. La trasformazione e il reporting, che rappresentano le azioni attraverso le quali è possibile visualizzare e manipolare i dati in accordo con gli obiettivi finali che hanno indotto il conseguimento delle informazioni.

Tali azioni, legate allo sfruttamento delle informazioni in possesso dalle imprese, sono percepite come funzioni particolarmente diffuse nell'economia moderna a cui il legislatore non resta disinteressato sia per promuovere lo sviluppo commerciale che, d'altra parte, per tutelare i singoli da abusi o distorsioni derivanti dall'impiego di questi strumenti, tanto da giustificare un ampio progetto legislativo di tenore internazionale.

Come già sottolineato, l'interazione alla base del fenomeno digitale vede oggigiorno dotarsi di una diffusione pervasiva e globale capace di collegare e implementare le relazione già esistenti tra le diverse nazioni. Dal punto di vista europeo viene data profonda importanza ai legami e agli scambi di informazioni che sono sostenuti con gli Stati Uniti, il prevalente alleato commerciale dell'Unione Europea. I due partner, infatti, cooperano strettamente e basano il loro rapporto sulla condivisione di ideali comuni quali la democrazia, la protezione e la salvaguardia dei diritti fondamentali dei propri cittadini, le libertà economica e politica. In quest'ottica, tra le due super potenze si sono susseguiti numerosi negoziati tali da rendere effettivi gli accordi globali nell'ambito del libero scambio e sfruttare integralmente le opportunità derivanti dalla loro relazione commerciale.

In aggiunta, l'urgenza e la crescente attenzione che vengono dedicate a questo tema complesso emergono decise in correlazione alle vicende che hanno visto protagonista Edward Snowden il quale, nel giugno 2013, rivela diverse informazioni inerenti a programmi di intelligence secretati statunitensi. Alla luce di tali divulgazioni, Maximilian Schrems cita in giudizio, nel giugno del 2014, Facebook Ireland Ltd.

Schrems assume in prima istanza che gli Stati Uniti non pratichino sufficienti misure per la protezione dei dati sensibili e perciò, in tale quadro, non si dimostrino partner idonei alla trasmissione di informazioni generate da utenti di piattaforme digitali europei. Si mette pertanto in discussione l'accordo esistente tra Usa e Unione Europea sul trasferimento di informazioni personali da un continente all'altro (il Safe Harbor, 2000), affermando che lo stesso viene violato ripetutamente e che nello specifico il social network Facebook si trova in possesso di una pluralità di informazioni riguardanti i propri utenti le quali non vengono eliminate nemmeno nel momento in cui il singolo decide di disiscriversi. Il clima di incertezza che ne è scaturito ha spinto le maggiori potenze mondiali a interrogarsi sui temi di sicurezza dei dati personali e su quale sia il livello di protezione adeguato degli stessi per garantire i diritti fondamentali degli individui. Tale dibattito convince l'Unione Europea ad intervenire per disegnare un sistema di supervisione più organico e per promuovere il rispetto di un insieme di garanzie. Inoltre, si è reso necessario assicurare che la fiducia che intercorre tra i partner commerciali non venisse intimidita dal contesto circostante affinché i flussi commerciali non fossero influenzati negativamente e le transazioni transatlantiche non fossero messe in discussione. È possibile affermare che questi due eventi hanno sovvertito l'apparente equilibrio che caratterizzava il contesto in cui le transazioni commerciali potevano farsi forza della libertà con cui le imprese entravano in possesso delle informazioni personali degli individui e ne facevano uso.

In questo quadro incerto, si rende necessario considerare l'intensità e l'entità delle informazioni che, alla luce degli intensi rapporti commerciali che intercorrono tra Unione Europea e Stati Uniti, quotidianamente vengono trasferite tra le imprese dotate di piattaforme digitali da una sponda all'altra dell'Atlantico. È quindi considerata come rilevante l'esigenza di conseguire un quadro normativo chiaro ed organico; infatti, in questa direzione, la Commissione Europea ha intensificato il processo negoziale con gli Stati Uniti per definire una base normativa rinnovata, completa e sicura.

3. LA PROTEZIONE DEI DATI IN EUROPA E NEGLI STATI UNITI

Come precedentemente affermato, un punto di condivisione trasversale che si riscontra nel rapporto tra Unione Europea e Stati Uniti è rappresentato dalla volontà e dall'impegno nel garantire i diritti fondamentali dei propri cittadini e, in questo frangente, assume un'importanza considerevole la determinazione profusa nell'assicurare il livello adeguato di sicurezza alla protezione dei dati personali, in particolar modo i dati provenienti da piattaforme elettroniche. Osservando la questione da un altro punto di vista si nota la difficoltà delle due potenze nel trovare uno schema legislativo condiviso. Le contrarietà nel trovare una base comune sono state associate alla dissomiglianza nella trattazione della materia da parte di Ue e Usa; le conseguenze che ne sono scaturite hanno avuto considerevole effetto nelle relazioni economiche tra le due potenze e sono state origine di *impasse* nei loro rapporti. Si può ottenere un raffronto in merito prendendo in considerazione le condizioni sottostanti la manipolazione dei dati personali. A titolo di esempio, la normativa americana non limita le imprese nell'esportazione di dati a paesi terzi, generalmente, quindi, l'Unione Europea non trova corrispondenza con le misure adottate in territorio statunitense.[6] Sebbene appaia confermata la determinazione a convergere ad una base di principi condivisa, le profonde differenze di concezione della protezione dei dati fanno presumere che questi sforzi saranno in qualche misura limitati.

Le difformità nell'analisi e nella trattazione della materia vedono la loro genesi in motivazioni di carattere culturale e storico che hanno condotto Unione Europea e Stati Uniti ad avvicinarsi al tema della protezione dei dati personali in modo del tutto differente. Il punto su cui si focalizzano gli Stati Uniti è l'equilibrio nazionale nel suo complesso; perciò l'accesso ai dati personali dei singoli viene consentita e la sicurezza degli stessi talvolta messa in secondo piano al fine di perseguire un obiettivo di carattere collettivo. Per quanto concerne l'Unione Europea, invece, l'attenzione viene posta in prima analisi sull'esigenza di tutelare i diritti fondamentali dei cittadini, le loro libertà e la tutela delle loro informazioni personali sensibili; solo in seguito al soddisfacimento di questi obiettivi si focalizza l'impegno sulla sicurezza complessiva degli stati membri. È bene sottolineare che nessuno dei due approcci è da biasimare: si tratta di due forme diverse di approssimarsi a una tematica in larga parte inesplorata la quale sta prendendo piede solo in tempi recenti e di cui, perciò, è ancora difficile farsi un'idea complessiva chiara e unitaria. Questi approcci, sebbene divergenti,

[6] Ioanna Tourkochoriti, The Snowden Revelations, the transatlantic trade and investment partnership and the divide between U.S.-Eu in Data privacy protection

trovano una loro stabilità e una sorta di bilanciamento fino al momento in cui non emergono le sconcertanti rivelazioni di Snowden e la successiva battaglia legale di Schrems.

3.1 L'APPROCCIO EUROPEO

Fin dalla sua genesi l'Unione Europea si ispira ai valori della coesione, del rispetto della dignità umana, della libertà, della democrazia, dell'uguaglianza, ideali che condizionano profondamente l'approccio con cui la Ue si avvicina ai diritti fondamentali degli esseri umani.

Con la Carta dei diritti fondamentali[7]il Consiglio, il Parlamento Europeo e la Commissione proclamano congiuntamente un documento che riunisce in un unico testo i diritti civili, politici, economici, sociali e societari fino a quel momento riportati in fonti diverse di carattere internazionale, nazionale, europeo. Attraverso il nuovo Trattato si vuole privilegiare una visione dell'Europa collettiva che allo stesso tempo non vuole trascurare gli interessi degli individui.

Assume particolare rilevanza il Capo II che si compone di quattordici articoli dedicati alle libertà tra cui spicca il diritto alla protezione dei dati personali. La Ue, infatti, considera la privacy delle comunicazioni e la protezione dei dati personali come un diritto essenziale, tanto da essere incorporati negli articoli 7 e 8 del Trattato; a sottolinearne la basilare importanza è anche il Trattato di Lisbona del 2007 (entrerà in vigore nel 2009) nel quale viene nuovamente attribuita attenzione alla cura della sicurezza dei dati personali.[8]

Fra i vari intervanti normativi il primo passo ad essere compiuto in tale direzione avviene nell'ottobre del 1995 quando l'Unione Europea giunge ad un accordo per armonizzare le differenti legislazioni nazionali in materia di sicurezza dei dati con la Direttiva sulla Protezione dei Dati (DPD)[9]. Si tratta di un provvedimento del tutto avveniristico che considera il ricorso sempre più frequente da parte della Comunità al trattamento di dati personali nei vari settori delle attività economiche e sociali, non tralasciando nemmeno i progressi registrati dalle tecnologie dell'informazione le quali facilitano notevolmente il trattamento e lo scambio di tali dati. Il DPD stabilisce una base di regole comuni, sia per enti pubblici che per quelli privati, da mettere in atto in tutti gli stati facenti parte l'Unione i quali trattengono o trasmettono dati personali. L'obiettivo che

[7] Pubblicata nella sua versione definitiva in GUCE 2000/C 364/01 il 18 dicembre 2000.
[8] Trattato di Lisbona modificativo del Trattato sull'Unione Europea e del Trattato costitutivo della Comunità Europea, 13 Dicembre, 2007, O.J. (C306).
[9] Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

si propone è quello di eliminare gli ostacoli alla circolazione dei dati personali stabilendo un elevato livello di tutela dei diritti e delle libertà delle persone in relazione al trattamento di tali dati nella Comunità. Il DPD si auspica di facilitare i flussi di informazioni nel territorio europeo, rafforzare il mercato interno e promuovere una economia comune basata sulle informazioni condivise. Si ritiene di specificare che tali principi di tutela enunciati sono applicati a tutti i trattamenti di dati personali in forma di suoni e immagini relativi a persone fisiche quando le attività del responsabile del trattamento rientrano nel campo di applicazione del diritto comunitario. Questa Direttiva si occupa di stabilire le modalità con cui le informazioni riguardanti i cittadini europei possono essere raccolte, trasformate, utilizzate e trasmesse da parte di tutte le entità che ne siano interessate e che ne vengano in contatto. Da un canto, quindi, sono sanciti gli obblighi a carico delle persone, autorità pubbliche, imprese, agenzie o altri organismi i quali si dimostrano responsabili delle trasformazioni ponendo particolare attenzione alla qualità dei dati, alla sicurezza tecnica, alla notificazione all'autorità di controllo, alle circostanze in cui il trattamento può essere effettuato; dall'altro si puntualizza il diritto delle persone, i cui dati sono oggetto di trattamento, di essere informate, di poter accedere ai dati stessi e chiederne la rettifica o di opporsi alla loro manipolazione. Un ulteriore aspetto su cui si focalizza la Direttiva è la disposizione di una linea di comportamento da adottare con gli stati estranei l'Unione ai quali viene fatto obbligo di rispettare determinate condizioni di sicurezza affinché possano entrare in contatto con i dati personali dei cittadini europei. In particolare, è permesso trasferire informazioni a paesi terzi solo se la Commissione Europea stabilisce che lo stato preso in considerazione fornisce un adeguato livello di protezione dei dati stessi. L'adeguatezza del livello di sicurezza viene valutata con riguardo alla natura delle informazioni, allo scopo e alla durata delle operazioni di trasformazione, alle nazioni di origine e a quelle di destinazione, ma soprattutto in base alle leggi, alle regole e a tutte le misure di sicurezza che vengono adottate dal paese.

Con l'adozione del DPD, si dispone che le informazioni possono essere raccolte ed usate solo per scopi specifici, espliciti e legittimati. Particolare attenzione è riservata ai dati sensibili riguardanti la razza, l'etnia di origine, credenze politiche o religiose, lo stato di salute e la vita sessuale. A questo scopo, la Direttiva richiede la creazione, in ogni stato membro, di Agenzie per la Protezione dei Dati (DPA). Si rende esplicito che a queste autorità deve essere accordata la possibilità di disporre dei mezzi necessari all'adempimento dei loro compiti, attraverso poteri di intervento o investigativi, nelle fattispecie in cui si verifichino reclami operati dai singoli individui; inoltre, viene attribuita a queste cariche il potere di intraprendere azioni legali tali da contribuire alla trasparenza dei trattamenti effettuati nello Stato membro da cui dipendono. La Direttiva dà disposizione che, a livello comunitario, deve essere inoltre costituito un gruppo per la tutela degli individui con

riguardo al trattamento dei dati personali che eserciti in piena indipendenza la sua funzione di consigliare la Commissione e di contribuire all'applicazione omogenea delle norme nazionali. Infine, si concede agli Stati membri un termine non superiore ad anni tre per il recepimento della Direttiva e per l'applicazione progressiva dei principi enunciati nella stessa a tutti i trattamenti e manipolazioni realizzati a partire dalla sua entrata in vigore.

3.2 L'APPROCCIO STATUNITENSE

Il diritto, negli Stati Uniti, si basa innanzitutto sulla fonte principale rappresentata dalla Costituzione e, sotto di essa, deriva dalle leggi promulgate dal Congresso e i molteplici Trattati a cui gli Stati Federali hanno la possibilità volontaria di aderire. Tenendo conto di tale struttura normativa, si rileva la carenza di un apparato unitario e organico. In particolare sembra essere in difetto un apparato legislativo completo dedicato alla protezione dei dati personali. Viene dato, infatti, ampio spazio di manovra agli Stati Federali i quali hanno la facoltà di creare diritto su tutte le materie che non rientrano già nel campo di applicazione della Costituzione o delle leggi federali. Si crea quindi una sostanziale differenza tra i diversi ordinamenti e si percepisce la mancanza di una struttura armonica e condivisa lungo tutto il territorio. In aggiunta, questo orientamento ha portato, nel corso del tempo, ad una stratificazione legislativa che in alcuni casi ricopre in modi diversi lo stesso problema trattato e in certi altri presenta delle vere e proprie lacune. Alcuni fanno riferimento a questo approccio definendolo un *patchwork* di leggi federali disconnesse tra loro, alimentando la necessità di avere una legislazione globale ed esauriente. Altri, per contro, sostengono che questo criterio adottato dagli Stati Uniti sia più agile e svelto rispetto a quello in vigore in Unione Europea e che permetta di sostenere e di promuovere le innovazioni americane in

campo tecnologico.[10]

È possibile affermare che l'orientamento seguito dagli Stati Uniti sia quello di assecondare le esigenze emergenti a livello territoriale e, solo successivamente, viene calata l'attenzione sulla tutela del singolo. Si sostanzia in questo modo un sistema legislativo insufficiente a rispondere a tutte le necessità che possono essere ricollegate a una giurisdizione di tale vastità. L'incertezza che ne scaturisce grava in maniera particolare ogniqualvolta si stringano rapporti con terze economie, mettendo in discussione la realizzabilità delle relazioni, siano esse di tipo economico, politico o

[10]Congressional Research Service, Martin A. Weiss, Kristin Archick , U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield

sociale. In aggiunta, la differenza sostanziale che si riscontra in relazione all'approccio messo in atto dall'Unione Europea concerne le misure di sicurezza implementate le quali distinguono tra cittadini americani e cittadini non-americani. In particolare, tale discordanza appare considerevole con riguardo ai programmi di sorveglianza di massa. La tendenza osservata è allora quella di affidarsi a Trattati e Direttive predisposti da altri organismi internazionali e ratificarne i risultati al fine di permettere, garantire e tutelare la liceità e la sussistenza del rapporto.[11] Un esempio è rappresentato proprio dalla tutela dei dati personali. In mancanza di una precisa legiferazione in merito, gli Stati Uniti acconsentono a trovare un punto di incontro con il loro maggiore partner commerciale, l'Unione Europea, per garantire la fattibilità della trasmissione dei dati personali negli scambi transatlantici tra le due potenze. L'accordo arriva nel 2000 quando Unione Europea e Stati Uniti concludono il Safe Harbor il quale consente il libero trasferimento, ai fini commerciali, dei dati dei cittadini europei verso gli Stati Uniti operati dalle multinazionali europee. Tale accordo regola le modalità attraverso le quali è acconsentito alle società statunitensi di esportare e gestire le informazioni personali dei cittadini europei.[12]

[11] Policy Department C, Citizens' rights and Constitutional affairs, A comparison between US and EU Data Protection Legislation for Law Enforcement,
http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf
[12] Internet Law, Dr. Nora Ni Loidean, The end of Safe Harbor: Implications for EU Digital Privacy and data protection law.

4. IL SAFE HARBOR AGREEMENT [13]

Gli approcci estremi adottati dalle due potenze per la tutela dei dati, convinsero Unione Europea e Stati Uniti della necessità di prevedere un meccanismo che permettesse alle aziende americane di incontrare gli standard di sicurezza richiesti dal DPD del 1995. Il timore di un possibile indebolimento dei rapporti commerciali e la minaccia di una profonda influenza negativa per numerosi business e industrie per ambedue lati dell'Atlantico, condussero, nel 2000, il Dipartimento del Commercio degli Stati Uniti a rilasciare i "Safe Harbor Privacy Principles",[14] ratificati poi dalla Commissione Europea[15]. Inoltre, in accordo con la decisione della Commissione Europea, i principi racchiusi nel Safe Harbor possono essere limitati nella misura in cui garantiscono i livelli di sicurezza nazionale, di pubblico interesse e incontrano i requisiti di legge. Questi principi vennero sviluppati principalmente con la finalità di prevenire la divulgazione o la perdita di informazioni personali dei cittadini da parte di società situate nei territori dell'Unione Europea o degli Stati Uniti.

La partecipazione all'accordo venne aperta ad ogni impresa americana assoggettata alla regolamentazione dalla Commissione Federale del Commercio (FTC). Nel luglio del 2000, la Commissione Europea riconobbe alle società americane aderenti allo schema disciplinato dal Safe Harbor di incontrare i requisiti di adeguatezza del livello di protezione dei dati riferiti ai cittadini europei. Sulla base del Safe Harbor, infatti, un'impresa americana interessata all'utilizzo di informazioni sui consumatori, aveva la possibilità, con cadenza annuale, di auto-certificarsi presso il Dipartimento del Commercio il quale dava conferma che la stessa organizzazione incontrasse i requisiti di base enunciati nell'accordo ed altresì incontrasse gli standard di sicurezza e tutela richiesti dalla normativa europea per la protezione dei dati.

[13] http://www.export.gov/safeharbor/

[14] U.S. Department of Commerce, Safe Harbor Privacy Principles and Related Frequently Asked Questions, July 21, 2000

[15] Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000.

4.1 I CONTENUTI, L'APPLICAZIONE, LE MOTIVAZIONI SOTTOSTANTI

Il Safe Harbor Agreement si basava sostanzialmente sull'emanazione di sette principi:

NOTICE – gli individui dovevano essere informati riguardo la raccolta delle loro informazioni e delle modalità con cui le stesse sarebbero state utilizzate. Inoltre, le imprese dovevano fornire tutte le indicazioni necessarie affinché i consumatori potessero entrare in contatto con i propri dati personali e, nel caso li ritenessero imprecisi o erronei, era accordata loro la facoltà di querelare le imprese coinvolte.

CHOICE – agli individui doveva essere data la possibilità di scegliere se rinunciare o acconsentire alla raccolta dei dati confidenziali e alla loro successiva trasformazione da parte degli enti interessati.

ONWARD TRANSFER – il trasferimento dei dati a parti terze era permesso solo nei limiti in cui queste aderissero e rispettassero le adeguate misure per la protezione delle informazioni sensibili.

SECURITY – delle misure ragionevoli e degli sforzi sostanziali dovevano essere messi in atto per prevenire la perdita o la rivelazione delle informazioni raccolte.

DATA INTEGRITY – i dati dovevano essere attendibili e pertinenti allo scopo con cui venivano raccolti.

ACCESS – agli individui doveva essere consentita la possibilità di accedere alle proprie informazioni personali e, nel caso queste venissero considerate inappropriate o errate, l'opportunità di correzione o eliminazione doveva essere garantita.

ENFORCEMENT – si riteneva necessario mettere in atto delle misure effettive operative per applicare questi principi.

Questi sette principi vennero studiati al fine di prevenire ogni possibile perdita o rivelazione di informazioni personali. Nel luglio del 2000 la Commissione Europea stabilì che agli enti americani, pubblici o privati, che si conformavano ai principi e che avevano ottenuto la certificazione del rispetto delle misure di sicurezza richieste era acconsentito il trasferimento dei dati aventi origine in Unione Europea; si faceva riferimento a questa conclusione come la Safe Harbor Decision.

Come affermato in precedenza, la particolarità di questo accordo era il fatto di non essere regolamentato a livello centrale dal governo statunitense. La Commissione Federale per il Commercio infatti si occupava di gestire e di coordinare il Safe Harbor e tutte le attività e prassi ad

esso correlate con la sovraintendenza del Dipartimento per il Commercio statunitense. Inoltre, si poteva identificare il Safe Harbor nella forma di una auto-certificazione che sottoponeva le imprese interessate a soddisfare determinate condizioni per poterne fare richiesta. In particolare, solo alle organizzazioni di origine statunitense assoggettate alla giurisdizione di competenza della Commissione Federale per il Commercio veniva concessa la possibilità di aderire all'Accordo.

5. IL CASO SCHREMS

Nel giugno del 2013 Edward Snowden rivela in via del tutto non autorizzata delle informazioni riguardanti i programmi di sicurezza dell'Agenzia per la Sicurezza Nazionale (NSA) degli Stati Uniti e altre notizie inerenti alle attività dell'intelligence americana. Riemerge, quindi, la preoccupazione attinente la tutela dei dati personali e, così, Unione Europea e Stati Uniti si trovano nuovamente ad interfacciarsi con una normativa che non permette di essere trascurata oltre e si confrontano sul livello di protezione e sicurezza necessari affinché le società americane possano proseguire nel raccogliere e utilizzare i dati originati nel territorio europeo e successivamente trasmessi alle loro sedi site in territorio statunitense. I timori avanzati dall'Unione Europa si dimostrano crescenti quando società di telecomunicazioni e di informazione americane risultano coinvolte nei programmi dell'Agenzia per la Sicurezza Nazionale (NSA), soprattutto con riguardo alle modalità di utilizzo dei dati personali e alle vaste possibilità di accesso del Governo statunitense alle informazioni stesse.[16]

Si lascia quindi spazio alla possibilità di interrogarsi quanto le proprie informazioni siano adeguatamente celate e protette e quale sia il livello di accesso ai dati considerato ammissibile al fine di non invadere irrimediabilmente la propria sfera personale e di non vedere violati i propri diritti fondamentali. Proprio in relazione a questo aspetto, il cittadino austriaco Maximillian Schrems concentra la sua attenzione sui livelli di sicurezza applicati ai dati personali degli 1,65 [17]miliardi di utenti del social network Facebook. Il focus della sua disputa risulta essere la tutela della sicurezza dei dati personali che emergono da piattaforme digitali, da social network e dalla molteplicità di software che tramite il web sono in grado di incamerare le informazioni e le attività afferenti ai navigatori.

Facebook, così come gli altri grandi colossi che si occupano di alta tecnologia quali Google e Microsoft, stabilisce i propri quartieri generali in Irlanda al fine di evitare di incorrere nel pagamento delle tasse americane misurate sui profitti esteri. D'altra parte, Facebook, adottando questa soluzione, rientra nel campo di applicazione del diritto europeo; questo aspetto si traduce nel fatto che a tutti gli utenti europei iscritti alla piattaforma devono essere garantiti gli stessi diritti di protezione accordati da qualsiasi altra società avente sede nei territori dell'Unione Europea. In particolare, gli utenti europei possono esercitare il diritto entrare in conoscenza di tutte le informazioni in possesso del social network. Al fine di sostenere la sua tesi Schrems, dopo averne

[16] https://edwardsnowden.com/impact/

[17] Dato aggiornato al 2016, www.panorama.it/mytech/social/facebook-numeri-impressionanti/

fatto richiesta, riesce ad ottenere un file in cui sono racchiuse tutte le attività e le azioni che egli stesso ha compiuto dal momento in cui ha deciso di iscriversi alla piattaforma, comprese quelle che risultano eliminate. L'immensa portata di informazioni che i database di Facebook conservano a riguardo dei loro iscritti convince lo studente austriaco della necessità di istituire un gruppo di attivisti cui viene dato il nome di "Europa v. Facebook" e intraprendere un'azione determinata a quantificare quale fosse la libertà di accesso ai dati degli utenti e comprendere il loro livello di protezione.

5.1 LA CAUSA ALLA COMMISSIONE PER LA PROTEZIONE DEI DATI (Europa vs Facebook)

Schrems riunisce una molteplicità di reclami e si indirizza verso la Agenzia per la Protezione dei Dati Irlandese attraverso la quale accusa il social network Facebook di immagazzinare e conservare nel tempo tutte le informazioni che gli utenti hanno tentato di eliminare dai propri profili. Inoltre si imputa responsabilità a Facebook di farsi possesso dei dati riguardanti i propri utenti e di convertirli nella forma di proprietà intellettuale. Il punto centrale su cui si focalizza la causa riguarda proprio il trasferimento di dati in possesso del social network Facebook dai suoi server situati in Europa alle altre piattaforme con base statunitense alla luce delle rivelazioni del giugno 2013 di Edward Snowden, il cosiddetto Prism Program. Nello specifico, l'imputazione sostenuta da Schrems asserisce che il regime sulla base del quale i dati personali dei cittadini europei sono trasferiti negli Stati Uniti da Facebook-Irlanda in accordo con l'auto-certificazione prevista dal Safe Harbor Agreement risulta incompatibile con la normativa dell'Unione Europea. Schrems ribadisce che le divulgazioni riguardanti il Prism Program danno prova del fatto che gli Stati Uniti non sono stati in grado di garantire che il trasferimento dei dati personali avvenga con un consono livello di sorveglianza.

La DPA irlandese, in prima istanza, rigetta la causa affermando che non sussistono basi che ne legittimino la stessa in ragione del fatto che Facebook aderisce al Safe Harbor Agreement. La DPA si trova, quindi, ad essere vincolata alla decisione della Commissione Europea secondo la quale tutte le società rientranti all'interno dell'accordo del 2000 garantiscono un adeguato livello di sicurezza alle informazioni di cui sono in possesso. Trascorso un anno di tempo dalla deposizione della prima causa, la sentenza rilasciata dalla Corte Suprema Irlandese (Irish High Court) si disgiunge dalla precedente conclusione a cui era arrivata la DPA Irlandese affermando, infatti, che

le motivazioni alla base della mozione sollevata da Schrems risultano fondate sia a livello nazionale che a quello comunitario.

In aggiunta, si mette in luce la difficoltà di rendere compatibili e attuali i principi espressi nel Safe Harbor in correlazione agli sviluppi legali e non legali che hanno visto susseguirsi dall'entrata in vigore dell'accordo stesso. Nello specifico, si fa riferimento all'impossibilità di accesso a un esame completo di dati. In relazione a questo aspetto si fa richiesta che il Safe Harbor Agreement e i suoi principi vengano allineati ed adeguati con la disciplina per la protezione dei dati personali in vigore nel territorio europeo.

Infine, un ulteriore aspetto su cui si porta l'attenzione riguarda la Corte Suprema Irlandese (Irish High Court) la quale fa richiesta alla Corte di Giustizia Europea di valutare la competenza in merito a questa causa da parte della DPA irlandese. Nello specifico si avanza pretesa di intendere se quest'ultima ha la facoltà di investigare su i livelli di sicurezza messi in atto da Facebook o, se, al contrario, si deve attenere alle decisioni prese dalla Commissione Europea, quindi se, in merito al caso specifico, si deve attenere al Safe Harbor Agreement.

5.2 IL LIVELLO DI PROTEZIONE ADEGUATO

Successivamente lo svolgimento dei fatti riguardanti Snowden prima e Schrems poi, il punto chiave su cui si pone l'attenzione è rappresentato dalla comprensione di quale possa essere il livello di sicurezza adeguato a garantire la tutela degli individui e la protezione dei loro dati personali. In questo frangente si prendono quali punti di riferimento gli articoli 7[18] e 8[19] della Carta dei Diritti Fondamentali dell'Unione Europea, i quali rappresentano il punto di avvio per innalzare il grado di protezione da implementare.

Gli aspetti da non sottovalutare nella trattazione dei livelli di sicurezza consoni dei dati personali al nostro tempo fanno riferimento all'infinita e omnicomprensiva memoria che Internet possiede con

[18] Art. 7/Carta dei Diritti Fondamentali dell'Unione Europea (2000/C 364/01) **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. "

[19] Art. 8/Carta dei Diritti Fondamentali dell'Unione Europea (2000/C 364/01) **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."

riguardo alle informazioni degli individui e, inoltre, la sviluppata capacità e influenza che sono in grado di esercitare i motori di ricerca sulle identità e sulle vite private dei singoli.

Un grado di sicurezza può definirsi adeguato allorquando è idoneo a tutelare i singoli e le loro vite private da uno uso scorretto delle informazioni che se ne possono ricavare. È altresì fondamentale garantire la piena appropriabilità e gestione delle proprie notizie riservate affinché sia garantito il diritto fondamentale della protezione dei dati di carattere personale.

A partire dalla sentenza correlata al caso di Snowden, è ora possibile valutare qualsiasi circostanza, inerente la fornitura di dati personali e la relativa trasformazione, che si renda rea di infrangere delle libertà essenziali prendendo come fulcro i diritti fondamentali enunciati nella legge europea e riportati nella Carta.

D'altra parte, però, ci si interroga se queste condizioni avvertite come improrogabili siano effettivamente raggiungibili e implementabili senza arrecare danno a tutto quell'insieme di imprese non inserite nell'Unione Europea che cercano di entrare in contatto con le informazioni dei cittadini europei. Risulta quindi preminente comprendere se gli elevati standard ricompresi nella legislazione europea possano indebolire i rapporti con gli Stati Uniti e con le altre potenze mondiali qualora questi principi dovessero essere adottati e condivisi dalle diverse nazioni.

5.3 LA DECISIONE DELLA CORTE DI GIUSTIZIA EUROPEA E LE CONSEGUENZE DELLA SENTENZA

La Corte di Giustizia Europea prende la sua decisione il 6 Ottobre 2015. Le conclusioni a cui arriva portano a diversi risultati.[20] Innanzitutto, si chiarisce come le scelte prese dalla Commissione Europea non riducono lo spazio di manovra a disposizione delle DPA degli stati membri: queste mantengono i loro poteri e possono investigare e ricercare notizie in merito alle cause che vengono sottoposte loro. La Corte di Giustizia Europea infatti conclude che le DPA nazionali devono essere in grado di esaminare, con la più completa indipendenza, ogni causa riguardante i diritti e le libertà degli individui e per connessione anche l'accesso, l'utilizzo e la trasformazione delle loro relative informazioni.

[20] Court of Justice of the European Union, "The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid," press release, October 6, 2015.

Con riguardo al Safe Harbor Agreement, invece, la CJEU dichiara l'accordo invalido. Infatti, in relazione all'Articolo 25 del DPD, alla Commissione Europea è richiesto di esaminare le leggi locali o gli eventuali accordi in essere nei paesi terzi prima di fare delle affermazioni in merito al livello di adeguatezza delle misure per la protezione dei dati personali. La Commissione, a partire dall'entrata in vigore del Safe Harbor Agreement nel 2000 non attua alcuna di queste rilevazioni, né richiede modifica alcuna per le misure previste dall'accordo; per questa ragione tale decisione viene dichiarata invalida. Di conseguenza, il Safe Harbor non costituisce più la base per il rapporto transatlantico per la tutela dei dati personali che lega Stati Uniti ed Unione Europea; sebbene restino comunque in vigore altri metodi che definiscono le modalità di trasferimento delle informazioni quali le Standard Contractual Clauses (SCC) o le Binding Corporate Rules a cui le imprese interessate possono riferirsi.

In più, la CJEU afferma che dal punto di vista degli Stati Uniti, la sicurezza nazionale, il pubblico interesse e le necessità di rafforzamento delle leggi hanno goduto della precedenza rispetto ai principi dichiarati dal Safe Harbor, e per questo, le conflittualità tra le diverse fonti legislative hanno portato a trascurare i requisiti previsti dall'accordo transatlantico. La conclusione a cui si è giunti è stata quella di definire il Safe Harbor quale portatore di interferenze tra le autorità statunitensi e i diritti fondamentali delle persone i cui dati personali venivano trasferiti dall'Unione Europea agli Stati Uniti.

5.4 LE RISPOSTE IN MERITO DA PARTE DI EUROPA E STATI UNITI

A partire dalla fine del 2013, la Commissione Europea e gli organi incaricati degli Stati Uniti cominciano un profondo lavoro congiunto di revisione dell'accordo transatlantico al fine di prendere in considerazione e di meglio integrare i principi europei negli standard di protezione dei dati statunitensi, specialmente con riguardo alle così dette "crepe di Snowden".

Sia dalla sponda europea che da quella statunitense si consolida la convinzione della necessità di un nuovo e migliore Safe Harbor Agreement; inoltre, si individuano le maggiori aree di interesse da preservare nella gestione dei flussi informativi tra Europa e Stati Uniti:

1. La protezione dei dati personali lungo l'Atlantico: il punto focale e ineludibile resta l'urgenza di salvaguardare le informazioni che attraversano i due continenti;

2. La tutela di un rapporto continuativo nello scambio di informazioni, vista l'importanza strategica per lo sviluppo commerciale non è possibile ignorare oltremodo le esigenze inerenti alla celerità e alla sicurezza della trasmissione dei dati personali;

3. Un rapporto di lavoro collaborativo tra le rispettive autorità incaricate della tutela delle informazioni personali con la finalità di trovare nuovi meccanismi o vie alternative per il trasferimento dei dati negli Stati Uniti, punto cruciale per evitare possibili decisioni contraddittorie tra le diverse autorità nazionali e fornire a cittadini e società punti di riferimento intellegibili.[21]

In accordo con la decisione della Corte di Giustizia Europea, il "Gruppo di Lavoro ex art. 29" conferma che i trasferimenti di dati che si concretizzano in ragione del Safe Harbor sono da considerarsi invalidi. Si rende necessario quindi trovare degli accordi politici, legali e delle soluzioni tecniche che permettano lo scambio dei flussi informativi pur non tralasciando il rispetto dei diritti fondamentali. Una rivisitazione o una rinegoziazione del Safe Harbor Agreement viene considerata come essere parte di queste soluzioni.

> "If by the end of January 2016, no appropriate solution is found with the US Authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection autorithies are committed to take all necessary and appropriate actions, which may include coordinated enforcement actions."[22]

Infine, l'Articolo 29 Working Party stabilisce con la data del 31 Gennaio 2016 il termine ultimo per Unione Europea e Stati Uniti per raggiungere un nuovo accordo riguardante la rivisitazione del Safe Harbor Agreement.

[21] European Commission, "First Vice-President Timmermans and Commissioner Jourova's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems)," press release, October 6, 2015

[22] Article 29 Working Party, "Statement of the Article 29 Working Party", press release, 16 Ottobre 2015.

6. LE POSSIBILITA' PER LE IMPRESE INTERESSATE DURANTE IL CAMBIAMENTO

L'armonizzazione e la ricerca di organicità nell'impostazione dell'apparato legislativo ambisce ad assicurare una libera circolazione delle informazioni, dati personali inclusi, tra gli Stati Membri e, allo stesso tempo, proteggere con un alto livello di sicurezza tutti i singoli coinvolti. Per gli stati non facenti parte l'Unione europea, è proprio la direttiva 95/46/ec a garantire il livello di sicurezza richiesto. Senza i principi promulgati dalla stessa, gli alti standard di protezione potrebbero essere agilmente valicati, considerata anche la facilità con cui le informazioni si possono dislocare utilizzando i network internazionali.

In attesa del nuovo accordo, le imprese si trovavano di fronte alla necessità di affidarsi a strumenti giuridici alternativi al fine di valutare i contratti in essere con le controparti statunitensi e completare il trasferimento dei dati personali verso gli Stati Uniti. In questa prospettiva, venivano prese quali punto di riferimento le "Standard Contractual Clauses" e le "Binding Corporates Rules" approvate dalla Commissione Europea [23], infatti, l'articolo 26 della Direttiva Ce/95/46 statuisce che:

"*Uno Stato membro può autorizzare un trasferimento o una categoria di trasferimenti di dati personali verso un paese terzo che non garantisca un livello di protezione adeguato ai sensi dell'articolo 25, paragrafo 2, qualora il responsabile del trattamento presenti garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone, nonché per l'esercizio dei diritti connessi; tali garanzie possono segnatamente risultare da clausole contrattuali appropriate*".

Questa Direttiva rappresenta solo il primo passo messo in atto dalla Commissione Europea con lo scopo di ottenere delle soluzioni contrattuali che permettano lo scambio di informazioni senza limiti di scambio tra le diverse nazioni. In questa prospettiva, l'Organo Europeo dedicato, intende adottare delle Direttive separate indirizzate alle molteplici tipologie di trasferimenti.

[23] 2010/87/: Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

6.1 LE STANDARD CONTRACTUAL CLAUSES E LE BINDING CORPORATE RULES

Nel giugno del 2011 la Commissione Europea adotta un provvedimento che sancisce la clausole contrattuali standard capaci di assicurare l'adeguato livello di salvaguardia dei dati personali trasferiti dall'Unione Europea a stati terzi non facenti parte della stessa. Attraverso tale Decisione, gli stati membri si impegnano a riconoscere alle organizzazioni o alle imprese che includono le suddette clausole all'interno dei loro contratti di incontrare e soddisfare i requisiti necessari alla protezione dei dati sensibili. In accordo alla Direttiva (95/46/CE) per la protezione dei dati si richiede che tutti i dati trasferiti a nazioni esterne ai confini dell'Unione rispettino l'adeguato livello di sicurezza. L'adesione volontaria a queste clausole contrattuali è un maggiore strumento che viene messo a disposizione di organizzazioni e imprese per ottemperare alle proprie obbligazioni.

Le Standard Contractual Clauses consistono di un apparato legislativo nel quale attraverso una dichiarazione legale vincolante ("warrant"), sia l'" Esportatore di Dati" che l'" Importatore di Dati" si assumono l'impegno di convertire le notizie sugli individui in informazioni attenendosi alle basilari regole per la protezione dei dati e concordano sul fatto che i singoli abbiano la facoltà di esercitare la loro forza contrattuale sotto questo accordo.

La disposizione a cui giunge la Commissione Europea obbliga quindi gli Stati Membri a riconoscere le clausole contrattuali annesse al provvedimento come rispettanti gli adeguati livelli di salvaguardia dei dati personali e come adempienti alla Direttiva per il trasferimento dei dati a paesi esterni i confini dell'Unione. Ciò nonostante, le Standard Contractual Clauses non assumono né un carattere obbligatorio per le imprese, né tantomeno sono l'unica soluzione legale che può essere adottata per il trasferimento a nazioni terze. Queste forniscono una possibilità ulteriore a quelle già comprese nella Direttiva per la Protezione dei Dati, la quale considera una molteplicità di situazioni concrete in cui i dati vengono trasferiti a paesi che non incontrano gli standard di sicurezza richiesti[24]. In aggiunta, le autorità di sicurezza per la protezione dei dati degli Stati Membri, godono dell'opportunità di autorizzare i trasferimenti delle informazioni valutando le circostanze del rapporto caso per caso, sempre che i dati beneficino delle appropriate soglie di sicurezza.

Si ritiene di sottolineare che le Contractual Clauses non sono condizioni richieste nelle occasioni in cui i paesi terzi presi in considerazione sono Svizzera o Ungheria, dei quali i rispettivi livelli di sicurezza sono stati reputati come confacenti gli standard richiesti dalla Commissione Europea.

[24] Esempio ne sono le casistiche in cui gli individui hanno fornito il loro consenso affinché i loro dati possano essere trasferiti fuori dall'Unione Europea e fattispecie in cui il trasferimento è necessario per la conclusione della performance o del contratto nell'interesse dei soggetti a cui i dati si riferiscono.

Un ulteriore strumento di natura contrattuale che garantisce la legittimità e l'affidabilità dei trasferimenti dei dati al di fuori del territorio europeo indicato dal Gruppo di Lavoro Ex Art. 29 è rappresentato dalle Binding Corporates Rules. Tali regole di comportamento racchiudono una serie di clausole che stabiliscono i principi vincolanti al cui rispetto sono tenute tutte le società afferenti ad un unico gruppo di impresa.

Si tratta di uno strumento ricettivo delle regole e degli adempimenti cui gli enti interessati devono fare riferimento; non rappresentano quindi un espediente capace di sostituire la normativa vigente in materia di tutela e trasferimento dei dati personali. Nonostante, quindi, tali clausole non siano investite della forza di legge, il loro contenuto viene abitualmente applicato dai Garanti europei allorquando si presentino le necessità di concessione delle autorizzazioni nazionali al trasferimento dei dati personali e soprattutto nell'eventualità di interpretazione della normativa vigente.

L'oggetto primo cui fanno riferimento le BCR consiste nei flussi di dati personali tra le società afferenti al medesimo gruppo di impresa le quali sono localizzate in diversi paesi del mondo; in questa direzione è possibile affermare che l'autorizzazione al trasferimento transfrontaliero delle informazioni personali sulla base di tali clausole trova una sua utilità nel momento sia rilasciata da tutte le Autorità di protezione dei dati da cui hanno origine i trasferimenti.

Con riferimento al contenuto delle stesse clausole viene richiesto che comprendano i principi guida sanciti dalla normativa per il trattamento dei dati personali infragruppo. Si rende perciò obbligatorio menzionare le finalità che si intendono perseguire sia attraverso il trasferimento dei dati personali che attraverso il loro trattamento generale. Inoltre, dovranno essere presenti le basi legali che legittimano ogni trattamento del dato personale le quali possono definirsi nel consenso rilasciato da parte del soggetto interessato, oppure nelle condizioni di esonero così come previsto dall'articolo 7 della Direttiva.

Nel momento in cui il gruppo sarà in grado di garantire le misure di sicurezza individuate dalla normativa, lo stesso sarà tenuto ad assicurare: (i) la predisposizione di un percorso di preparazione del personale in materia di protezione dei dati personali; (ii) l'implementazione di un sistema per la gestione degli eventuali contenziosi che potrebbero derivare da segnalazioni connesse alle BCR; (iii) la trasmissione periodica di audit al fine di valutare il rispetto delle clausole da parte delle società del gruppo; (iv) la creazione di uno staff dedicato al monitoraggio del rispetto delle BCR.[25]

[25] http://www.consulentelegaleinformatico.it/2015/11/18/binding-corporate-rules-e-trattamento-dati-come-applicarle-in-azienda/

7. IL PRIVACY SHIELD AGREEMENT

La Corte di Giustizia Europea, con la sua decisione del 6 Ottobre 2015, rende definitivamente invalido il Safe Harbor Agreement. Il precedente accordo viene soppiantato da un nuovo trattato che prevede maggiori obbligazioni a carico delle organizzazioni americane che vogliono utilizzare dati ed informazioni aventi origine da piattaforme digitali situate nei territori dell'Unione Europea; perciò, al fine di garantire una protezione maggiore degli stessi dati e attuare un più rigido monitoraggio si rende fondamentale una intensa cooperazione tra il Dipartimento del Commercio americano, la Commissione Federale del Commercio (FTC) e l'Autorità Europea per la Protezione dei Dati. Il nuovo accordo per il flusso di dati transatlantici e per la riservatezza degli utenti online dell'Unione Europea prende il nome di Privacy Shield e tiene in considerazione il nuovo contesto internazionale in ambito tecnologico ed informativo; in particolar modo pone attenzione all'emergenza legata ai big data e al correlato crescente bisogno di chiarezza per il business in rete. Il Privacy Shield viene approvato il 12 luglio 2016 e diventa effettivo con decorrenza 1 agosto 2016. A partire da tale data le imprese hanno la possibilità di aderirvi; viene affidato al Dipartimento del Commercio degli Stati Uniti l'incarico di verificare l'effettiva osservanza degli alti standard di sicurezza per la protezione dei dati operata dagli enti sottoscriventi.

"The EU-U.S. Privacy Shield protects the fundamental rights of Europeans and ensures legal certainty for businesses, including European companies, transferring personal data to the U.S. The Privacy Shield ensures easier redress for individuals in case of any complaints. I am therefore confident that the Privacy Shield will restore the trust of Europeans in the way their personal data are transferred across the Atlantic and processed by companies there. I encourage companies to sign up and I invite citizens to find out about their rights under the Privacy Shield in the 'citizens' guide' we are publishing today".[26]

[26]Věra **Jourová**, the EU's Commissioner for Justice, Consumers and Gender Equality, http://ec.europa.eu/justice/newsroom/data-protection/news/160801_en.htm

7.1 I NUOVI CONTENUTI, L'APPLICAZIONE E I MIGLIORAMENTI

L'obiettivo chiave che si propone il nuovo accordo è quello di avere la certezza di garantire un livello equivalente di protezione dei dati: non si aspira ad una mera copia dell'apparato legislativo europeo, piuttosto, con il Privacy Shield, si auspica una raccolta dei principi fondamentali e perciò, si rende esplicita la volontà di assicurare un livello di sicurezza fuori i confini del territorio dell'Unione essenzialmente paragonabile a quello all'interno della stessa.

Si ritiene di specificare che quando si fa riferimento all'"adeguato livello di sicurezza", sebbene non si faccia richiesta al paese terzo di predisporre delle misure e delle garanzie identiche a quelle presenti nell'Unione Europea, di fatto si richiede, in ragione delle normative vigenti nel territorio dello stato considerato e alla luce degli accordi internazionali pattuiti, un livello di protezione dei diritti fondamentali e delle libertà dell'individuo che sia equiparabile alla soglia assicurata all'interno dell'Unione Europea in virtù della Direttiva sulla protezione dei dati personali.

In questa direzione vengono perciò designate quattro aree da implementare al fine di permettere una più solida garanzia per le informazioni personali degli utenti:

1. La lavorazione dei dati deve avvenire attraverso delle regole di comportamento e di procedura chiare, specifiche e accessibili. In questo modo, viene acconsentito agli individui di sapere esattamente come vengono processati i dati che li riguardano.
2. Devono essere chiare le finalità con cui queste informazioni vengono raccolte, inoltre, le stesse intenzioni devono essere dimostrate. È richiesto un valido motivo per accedere alla sfera personale degli individui e per invaderne i diritti fondamentali, tale motivo deve essere bilanciato e proporzionato all'obiettivo che si intende raggiungere attraverso la raccolta di informazioni.
3. Viene considerato come necessario un organismo *super partes* indipendente e neutrale che abbia le facoltà e la libertà di intervenire con i controlli utili nel caso in cui se ne verifichi l'esigenza.
4. Si rende utile predisporre dei rimedi effettivi da mettere a disposizione degli individui affinché sia garantito ad ogni singolo il diritto di difendere i propri diritti attraverso l'attivazione di un corpo indipendente dedicato a tale scopo.[27]

Un punto dell'accordo ritenuto fondamentale è l'impegno preso da Europa e Stati Uniti nell'effettuare una revisione regolare e periodica dell'applicazione pratica del Privacy Shield.

[27] Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision

Inoltre, l'aspetto più incoraggiante è rappresentato dalla possibilità di partecipazione alla revisione del documento accordata ai rappresentanti delle autorità per la protezione dei dati personali. Infatti, un trattato che sappia stare al passo con i tempi, che sia capace di rinnovarsi a seconda delle esigenze emergenti e contestuali è basilare per raggiungere, da una parte, la piena tutela delle informazioni sensibili degli individui, e, dall'altra, il sostenimento necessario a un maggiore rafforzamento ed espansione dei rapporti commerciali transatlantici.

Le previsioni primarie che emergono dal nuovo accordo sono le seguenti:

- Maggiori obblighi per le società statunitensi. Sono previsti, infatti, dei rigidi vincoli affinché possa ritenersi garantita un'elevata trasparenza nel trattamento dei dati, dei meccanismi di vigilanza sulle attività delle organizzazioni statunitensi e la previsione di sanzioni o l'esclusione dal trattato stesso in caso di violazione di tali vincoli. Inoltre, sono predisposte condizioni più stringenti e rigorose nell'eventualità del trasferimento successivo dei dati personali a terze imprese.
- Al Governo degli Stati Uniti vengono applicati alcuni limiti all'accesso di massa ai dati personali: il suddetto deve essere tutelato da garanzie e obblighi di trasparenza. Attraverso meccanismi di controllo è proibito l'accesso generalizzato alle informazioni personali. Le garanzie sono applicate a tutte le fattispecie che coinvolgono il trasferimento dei dati personali negli Stati Uniti, anche se si tratta di accordi diversi dal Privacy Shield, come, ad esempio, le clausole contrattuali standard approvate dalla Commissione Europea (Standard Contractual Clauses) e le Binding Corporate Rules (BCR). Nell'adozione della suddetta soluzione si eviterà la comunicazione incontrollata di dati personali ad agenzie governative
- La protezione dei cittadini europei diventa effettiva con la possibilità di esercitare ricorso. Viene, in aggiunta, istituito un nuovo strumento di conciliazione nell'eventualità di possibili contenziosi tra Europa e Stati Uniti attraverso la creazione di un Ombudsman indipendente dalle autorità di vigilanza e sorveglianza munito del potere di gestione e risoluzione di controversie legati ai ricorsi da parte degli interessati, aventi sede nell'Unione Europea.
- Si predispone di un meccanismo annuale di riesame congiunto, il quale consente di monitorare il funzionamento del Privacy Shield, compresi gli impegni e le garanzie relative all'accesso ai dati ai fini di contrasto della criminalità e finalità di sicurezza nazionale. Infine, si rilascia alla Commissione Europea l'autorizzazione a pubblicare, con cadenza annuale, un rapporto indirizzato al Parlamento Europeo e al Consiglio dell'Unione Europea tale che si riferiscano le valutazioni compiute sullo stato di applicazione e sul rispetto dell'accordo, siano essi provenienti da contatti diretti, sia provenienti da altre sorgenti di

informazioni, come, a titolo di esempio, rapporti sulla trasparenza nel trattamento dei dati elaborati da enti coinvolti.

- Oltre a ciò, si ritiene necessario istituire molteplici modalità attraverso le quali estinguere le numerose cause di violazioni che si vedevano presenti sotto il Safe Harbor. Nello specifico, le imprese americane le quali si dedicano alla trattazione dei dati personali degli individui europei devono rispondere ai reclami avanzati dagli stessi entro un termine di 45 giorni. Deve essere, inoltre, reso disponibile un meccanismo alternativo di risoluzione del contenzioso senza oneri a carico dell'interessato. In aggiunta, viene considerato opportuno che l'autorità europea per la protezione dei dati collabori con il Dipartimento Americano del Commercio e con la Federal Trade Commission nell'ottica di garantire una rapida verifica e risoluzione dei contenziosi che non abbiano avuto un chiarimento con i canali testé menzionati.[28]

Prima della formale adozione, l'accordo è stato esaminato dal Gruppo di Lavoro Ex Articolo 29 per la protezione dei dati, un organismo consultivo indipendente composto da un rappresentante delle autorità nazionali di protezione dei dati personali, dal Garante europeo della protezione dei dati e da un rappresentante della Commissione Europea, e dal comitato dei rappresentanti degli Stati membri, presieduto da un rappresentante della Commissione Europea, previsto dall'Articolo 31 della Direttiva 95/46/CE sulla protezione dei dati personali. Il Gruppo di Lavoro art. 29 ha sottolineato che il Privacy Shield costituisce un miglioramento sostanziale in materia in relazione al precedente Safe Harbor contribuendo ad un maggior livello di tutela degli interessati.[29]

Sono tuttavia previste delle limitazioni all'applicazione delle misure previste dal del Privacy Shield:

a) Nella misura in cui risulti necessario andare incontro ad esigenze di sicurezza nazionale, pubblico interesse o fattispecie in cui si richiedano dei rafforzamenti dei requisiti di legge;
b) Nel caso in cui in base allo statuto o alla regolamentazione del governo un'organizzazione sia in grado di dimostrare che la non armonia con i principi previsti nel Privacy Shield porti a preferire le altre fonti all'accordo, avendo sempre quale finalità la tutela degli interessi delle persone;
c) Se delle deroghe o delle eccezioni sono compatibili al contesto in cui viene applicato il trattato.

[28] EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield Strasbourg, 2 February 2016

[29] https://www.digital4.biz/executive/law4digital/il-privacy-shield-verso-l-approvazione-definitiva_43672158372.htm

8. IL CONFRONTO TRA SAFE HARBOR AGREEMENT E IL PRIVACY SHIELD AGREEMENT

La crescente consapevolezza della capillare diffusione delle tecnologie dell'informazione e delle relative implicazioni che coinvolgono la gestione dei dati personali degli individui che ne fanno uso ha avuto uno slancio considerevole solo in tempi piuttosto recenti. Prima del concepimento del Privacy Shield, infatti, le esigenze correlate alla tutela delle informazioni private dei singoli venivano in qualche modo soddisfatte in modo frammentario e disomogeneo non considerando approfonditamente tutte le conseguenze che possono derivare da un incompleto quadro normativo in materia. Si ritiene opportuno sottolineare che di fatto la portata e gli ambiti collegati alla raccolta, la trasformazione e il riutilizzo dei dati personali sono fortemente incrementati da quando venne istituito l'originario Safe Harbor nel 2000. Risulta quindi necessario effettuare un confronto tra i due Trattati al fine di metterne in luce i maggiori aspetti critici e valutare se effettivamente i punti di stallo riscontrati nell'esecuzione del Safe Harbor possono considerarsi superati con l'entrata in vigore del Privacy Shield Agreement.

8.1 SAFE HARBOR AGREEMENT

Probabilmente, il maggiore punto debole che può essere attribuito al Safe Harbor Agreement si riferisce proprio alla sua natura di auto-certificazione, tanto è vero che ne sono conferma diverse occasioni in cui l'Unione Europea critica la sua applicazione e la sua disciplina.

Nel 2002, infatti, un controllo operato dall'Unione Europea rileva che un considerevole numero di imprese le quali dichiarano di essere in possesso della auto- certificazione rilasciata secondo le modalità previste dall'Accordo, nella realtà operativa non sembrano rispettare gli obblighi inerenti il livello di trasparenza in riferimento al contenuto espresso nelle loro politiche di tutela dei dati personali e alle modalità con cui i principi espressi dal Safe Harbor vengono applicati.

Successivamente, nel 2008, la società di consulenza australiana Galexia afferma che solo una minima parte di tutte le imprese rientranti nell'Accordo effettivamente garantisce l'adeguata cura delle informazioni personali dei cittadini europei. Nello specifico, Galexia imputa il mancato rispetto delle condizioni minime per la tutela dei dati personali a una incompleta comprensione dello schema normativo previsto dal Safe Harbor. Viene quindi consigliato all'Unione Europea, da

una parte, di rinegoziare l'intero accordo con gli Stati Uniti e in aggiunta di portare a termine una completa revisione di tutte le imprese facenti parte del patto; e vengono esortati gli Stati Uniti, dall'altra, di compiere una approfondita analisi volta a ricercare tutte le organizzazioni che fanno uso improprio della certificazione ottenuta sotto il Safe Harbor Agreement. La mancanza di coattività di adesione per tutte le imprese potenzialmente interessate e l'insufficienza di controlli e verifiche indirizzate alle entità auto-certificate portano, sostanzialmente, a disattendere le aspettative di tutela, correttezza e trasparenza concernenti la trasmissione dei dati personali. Si lascia, forse, troppo spazio all'autonomia delle imprese in un frangente che invece dovrebbe essere rigidamente normato e nel quale, soprattutto, dovrebbe essere attuato un controllo sistematico ed indifferenziato. La parziale imperizia con cui è stato predisposto questo accordo può essere ascritta alla difficoltà dell'apparato legislativo di prevedere lo sconfinato uso dei dati personali degli individui e le pluralità di usi e applicazioni che possono avere gli stessi nel momento in cui il Safe Harbor viene concepito e successivamente entra in vigore. Le implicazioni che ne derivano conducono gli Stati Uniti ad interfacciarsi con grandi cause legali di portata mondiale le quali sovvertono il sistema e inducono il legislatore ad abbandonare tale impostazione e ad introdurre significative innovazioni con riferimento alla struttura dell'accordo.

8.2 PRIVACY SHIELD AGREEMENT

Il pregio che può essere riconosciuto al Privacy Shield Agreement è quello di tenere in considerazione il mutevole contesto tecnologico mondiale. In questa prospettiva l'intento che ne emerge concerne la volontà di prevedere le future evoluzioni del settore, ciò si traduce nell'istituire delle misure maggiormente vincolanti per le imprese che rientrano nel campo di interesse del Trattato tali da garantire un livello di sicurezza sostanziale e tutelare i diritti fondamentali delle persone.

Inoltre, il Gruppo di Lavoro art. 29 riconosce al nuovo Accordo significativi miglioramenti asserendo che grazie alla negoziazione i maggiori difetti possono considerarsi superati. Nonostante ciò, viene fatto notare che permangono sostanziali lacune con riguardo ad alcuni aspetti chiave sia sul piano commerciale che a livello di sicurezza nazionale. Nello specifico:

- Difficoltà nel riscontrare quali siano le obbligazioni a carico degli enti i quali pervengano agli obiettivi che giustificano la raccolta dei dati personali. In questo quadro risulta se sia

necessario eliminare tutte le informazioni in proprio possesso una volta che non ne sia motivato l'utilizzo;

- Vengono tuttora considerate insufficienti le misure di sicurezza rivolte alla protezione dei dati coinvolti nel trasferimento a terze economie;
- L'accesso ai dati di massa da parte dei funzionari statunitensi non può definirsi idonea non incontrando gli standard per la protezione dei dati inerenti alla sorveglianza praticata dalle autorità pubbliche.

In aggiunta viene riscontrata una mancanza di chiarezza nei documenti che lo costituiscono. Si percepisce, infatti, una certa difficoltà nella consultazione dell'accordo dovuto alla presenza nello stesso sia dei principi fondamentali che degli allegati inerenti a molteplici campi di interesse. Risulta di primaria importanza che non si presentino situazioni di ambiguità o di fraintendimento nell'interpretazione del trattato affinché questo possa essere definito effettivo e ben funzionante per entrambe le parti. Inoltre, secondo il Gruppo di Lavoro art. 29, si percepisce una mancanza di chiarezza in merito a chi possa essere considerato effettivamente beneficiario della protezione garantita dal Privacy Shield; ovvero se possono essere reputati destinatari della tutela tutti i cittadini europei o, dall'altra parte, tutti i cittadini residenti all'interno dei territori dell'Unione Europea. Questo punto emerge come un aspetto da non trascurare in relazione al diritto di esercitare ricorso e alla presenza di meccanismi di auto-tutela che sono accordati agli individui a cui si indirizzano le misure di protezione dei dati personali.

Complessivamente si colgono diversi avanzamenti in materia grazie all'adozione del nuovo Trattato che risulta quindi più completo e pervasivo nonostante vengano riscontrati alcuni punti insicuri.

9. CONCLUSIONI

Con la recente entrata in vigore del Privacy Shield l'impressione che se ne ricava è rappresentata da un sostanziale avanzamento nella direzione di un quadro normativo organico ed esaustivo, ma da un altro punto di vista si ha la percezione che tale accordo manchi ancora di una effettiva applicabilità e di una garanzia per quanto concerne un livello di protezione adeguato alla tutela dei diritti fondamentali degli individui sia dal punto di vista del settore privato che di quello pubblico.

Va sin da subito osservato, in tale prospettiva, che le difficoltà maggiori possono essere riscontrate in particolar modo dai singoli utenti la cui difesa dei dati personali dovrebbe esprimere l'obiettivo primo di tale accordo. Si nota, in effetti, l'onerosità del procedimento di auto-tutela che deve essere messo in atto dall'interessato nel caso di contenzioso con l'organizzazione che fa uso dei suoi dati personali che di fatto parrebbe minare la attuabilità delle misure previste e di conseguenza la concreta protezione. Viene infatti vista come improbabile la via attraverso la quale, nella fattispecie in cui gli utenti europei considerino i propri diritti fondamentali violati, gli interessati debbano in prima istanza contattare gli organismi di arbitraggio statunitensi e le autorità nazionali che successivamente si occuperanno di contattare a loro volta le autorità statunitensi al fine di indirizzarsi verso l'impresa coinvolta nel contraddittorio. Il risultato che ne emerge vede la difficoltà di attuazione di effettive conseguenze per un ente che si dimostri reo di violare i diritti fondamentali degli utenti.

Un ulteriore aspetto su cui porre l'attenzione concerne il settore pubblico. In questa ottica, il Safe Harbor Agreement venne considerevolmente criticato dalla Corte di Giustizia Europea in relazione alla modalità con cui la legge statunitense si affaccia alla materia della sorveglianza di massa. Precisamente, i cittadini statunitensi possono godere di determinate protezione contro le misure adoperate per la sorveglianza di massa mentre i singoli non americani ne sono esclusi. La difficoltà si sostanzia nel fatto che neppure la versione finale del Privacy Shield adotta dei provvedimenti discostanti dal precedente Trattato; perciò, è possibile affermare che tale circostanza si trovi in contrasto con la tutela dei diritti fondamentali difesi dall'Unione Europea. Come conseguenza, la Corte Europea ha agito contro l'accesso di massa alle informazioni personali al fine di vedere rispettati i diritti alla privacy e alla protezione dei dati. Ugualmente, anche con riferimento all'ambito pubblico le forme di tutela che sono state predisposte sono considerate irrisorie in quanto si concretizzano in un Ombudsman statunitense, il quale non rappresenta un apparato indipendente bensì un sottosegretario del Governo degli Stati Uniti.

In questa prospettiva, si vede come necessaria una previsione nel Privacy Shield di una misura adatta a inibire l'accesso di massa ai dati personali, aspetto che viene considerato dall'Unione Europea come non compatibile con la tutela dei diritti fondamentali per la protezione dei dati.

Infine, con riferimento all'ambito commerciale, le misure e procedure confermate nel Privacy Shield pongono gli operatori europei su un piano svantaggiato rispetto alle imprese americane alle quali non è richiesto di incontrare gli alti standard di tutela dei dati personali dei propri utenti, si diffonde quindi la convinzione che questo accordo non soddisfi le esigenze di certezza che si sperava di raggiungere nel settore.

Per concludere, è possibile affermare che attraverso l'approvazione del Privacy Shield è stato compiuto il primo passo verso un quadro normativo in materia più completo ed esaustivo sebbene non sia ancora possibile affermare di aver raggiunto un accordo capace di tutelare gli utenti, proteggere l'accesso generalizzato e indiscriminato ai dati di massa e, in più, favorire e dare slancio alle relazioni commerciali transoceaniche. In questa direzione, infatti, una considerazione che può essere ragionevolmente avanzata consiste nell'interesse dell'Unione Europea a ritardare l'implementazione del Trattato fino a che il frangente statunitense non si commisuri alle disposizioni europee al fine di non assistere nuovamente all'invalidazione da parte della Corte di Giustizia Europea.[30]

[30] https://www.irishtimes.com/opinion/privacy-shield-the-new-eu-rules-on-transatlantic-data-sharing-will-not-protect-you-1.2719018

BIBLIOGRAFIA

ALBRECHT, J. P., SCHREMS, M., (2016), Privacy Shield: The new EU rules on transatlantic data sharing will not protect you, *The Irish Times, in:https://www.irishtimes.com/opinion/privacy-shield-the-new-eu-rules-on-transatlantic-data-sharing-will-not-protect-you-1.2719018*

ARTICLE 29 WORKING PARTY – Press release, (2015), Statement of the Article 29 Working Party

ARTICLE 29 WORKING PARTY, (2016), Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision, *in: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf*

BOEHM, F., (2015), A comparison between US and EU Data Protection Legislation for Law Enforcement,*in:http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536459/IPOL_STU(2015)536459_EN.pdf*

CARTA DEI DIRITTI FONDAMENTALI DELL'UOMO DELL'UNIONE EUROPEA 2000/C 364/01, (2000), *Art. 7 e 8, Pubblicata nella sua versione definitiva in GUCE 2000/C 364/01 il 18 dicembre 2000.*

CATANIA, R., (2016), Facebook: 30 numeri impressionanti, *Panorama, in: www.panorama.it/mytech/social/facebook-numeri-impressionanti/*

COMMISSION DECISION 2000/520/EC, (2000)

COMMISSION DECISION N. 2010/87/EU, (2010), On standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council

COURT OF JUSTICE OF THE EUROPEAN UNION – Press Release, (2015), "The Court of Justice Declares that the Commission's US Safe Harbour Decision Is Invalid,"

DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196, ART. 4 1. B), Codice in materia di protezione dei dati personali

DIRETTIVA 95/46/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, Relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati (1995)

DIRETTIVA N. 2002/58/CE DEL PARLAMENTO EUROPEO E DEL CONSIGLIO, (2002), Relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche)

EUROPEAN COMMISSION – Press release, (2015), First Vice-President Timmermans and Commissioner Jourova's Press Conference on Safe Harbor Following the Court Ruling in Case C-362/14 (Schrems)

EUROPEAN COMMISSION – Press Release, (Strasbourg, 2 February 2016), EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield

EXPORT.GOV, (2016, last updated), U.S.-EU & U.S.-Swiss Safe Harbor Frameworks, *in:http://www.export.gov/safeharbor/*

FAGGIOLI, G., GIORGINI, C., (2016), Il Privacy Shield verso l'approvazione definitiva, *Digital 4 Executive, in:https://www.digital4.biz/executive/law4digital/il-privacy-shield-verso-l-approvazione-definitiva_43672158372.htm*

FREDIANI, V., (2015), Binding Corporate Rules e trattamento dei dati: come applicarle in azienda, *Il Documento Digitale III/MMXV, in: http://www.consulentelegaleinformatico.it/2015/11/18/binding-corporate-rules-e-trattamento-dati-come-applicarle-in-azienda/*

GARANTE DELLA PRIVACY, (2014), Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati

GARANTE DELLA PRIVACY, (2015), Trattamento dei dati personali riferiti alla navigazione internet dei dipendenti

GARANTE DELLA PRIVACY, (2015), Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche

GARANTE DELLA PRIVACY, (2015), Trasferimento dati personali verso gli USA: caducazione provvedimento del Garante del 10.10.2001 di riconoscimento dell'accordo sul c.d. "Safe Harbor"

JOUROVÁ, V.,- PRESS RELEASE, (2016), EU-U.S. Privacy Shield fully operational from today, http://ec.europa.eu/justice/newsroom/data-protection/news/160801_en.htm

MARTIN A. WEISS, KRISTIN ARCHICK, (2016), U.S.-EU Data Privacy: From Safe Harbor to Privacy Shield, *Congressional Research Service, 7-5700 www.crs.gov R44257*

MINGHETTI, M., (2016), Era delle aziende piattaforma, *Supplemento allegato al n. 7/8 Luglio-Agosto 2016 di Harvard Business Review, in:http://marcominghetti.nova100.ilsole24ore.com/2016/07/18/era-delle-aziende-piattaforma/*

NORA NI LOIDEAN, (2016), The end of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law, *Journal of Internet Law, Vol.19, No. 8, February 2016*

THE COURAGE FOUNDATION, *Free Snowden, In support of Edward Snowden, in:https://edwardsnowden.com/impact/*

TOURKOCHORITI, I., (2014), The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide between U.S.-Eu in Data Privacy Protection, *University of Arkansas at Little Rock Law Review, vol. 36*

TRATTATO DI LISBONA, (2007), O.J. (C306).

U.S. DEPARTMENT OF COMMERCE, (2000), Safe Harbor Privacy Principles and Related Frequently Asked Questions