Introduzione

Scopo del presente lavoro è compiere una ricognizione e un'analisi delle regole che disciplinano il trasferimento dei dati personali dall'Unione europea verso Paesi terzi.

In particolare, si affronteranno alcune delle problematiche inerenti agli accordi sul trasferimento dati conclusi con gli Stati Uniti.

In linea generale, essi si basano sulla direttiva 95/46/CE, nucleo principale della normativa Ue sulla protezione e la circolazione dei dati personali, la quale prevede che un trasferimento di dati possa essere effettuato solo verso quei Paesi che garantiscono un livello di protezione adeguato.

Lo strumento principale per riconoscere tale livello di protezione e consentire di trasferire i dati è la decisione di adeguatezza che la Commissione europea può adottare verso quei Paesi che ritiene, appunto, adeguati.

Il tema del trasferimento dati verso paesi extra-Ue sta assumendo una crescente importanza per lo sviluppo che l'economia digitale ha comportato nell'epoca attuale.

È noto, infatti, che molti dei servizi e dei beni sono scambiati, da oltre vent'anni, tramite Internet e le moderne tecnologie dell'informazione.

Il trattamento dei dati e delle informazioni, nella maggior parte dei casi, avviene in altri Paesi rispetto a quelli in cui vengono raccolti o generati. È per questo motivo che il flusso di dati ha un enorme valore economico e commerciale, e spesso comporta rilevanti problemi giuridici in ordine alla sicurezza degli stessi e alle garanzie del diritto alla protezione dati degli utenti.

Analizzare il regime giuridico e gli accordi internazionali sul trasferimento dati permetterà quindi di capire se le garanzie e i diritti previsti dalle norme sulla protezione dati in Unione europea sono effettivi anche al di fuori dell'ordinamento europeo.

L'ambito metodologico comprenderà l'analisi della legislazione europea sulla protezione dati, avendo riguardo sia di quella di rango primario (come la Carta dei diritti fondamentali e i Trattati istitutivi), sia di quella secondaria, ossia direttive, regolamenti, decisioni.

Inoltre, si valuteranno i due principali accordi sullo scambio di dati conclusi dall'Unione europea con gli Usa: particolare attenzione sarà dedicata alla problematica della sorveglianza delle agenzie di intelligence e la conformità della loro attività ai principi della protezione dati così come stabiliti negli accordi stessi.

Le altre principali fonti saranno i pareri e i documenti ufficiali dei principali organi della protezione dati europei, come il "Gruppo articolo 29" e le autorità garanti nazionali.

Punto di partenza del lavoro sarà la sentenza resa il 6 ottobre 2015 dalla Corte di giustizia dell'Ue in un caso vertente una disputa fra l'azienda *Facebook* (piattaforma sociale on-line avente sede e fondata negli Stati Uniti e operante anche in Ue tramite una controllata stabilita in Irlanda) e un utente austriaco, il Sig. Schrems, il quale lamentava una non conformità della legislazione americana sull'intelligence con i principi dell'accordo sul trasferimento di dati personali (i c.d. *Safe Harbor pinciples* stipulati fra Ue e Usa nel 2000).

La disputa in questione trae origine dalle rivelazioni sui programmi di sorveglianza di massa effettuati dall'amministrazione Usa sui dati trattati dai "colossi del web" americani, denunciate nel 2013 dall'ex agente della *National Security Agency* Edward Snowden nel caso *Datagate*. Lo scandalo ha contribuito a fare luce sulla poca trasparenza e legittimità delle attività del settore dei servizi web, innescando una serie di interrogativi sulla sicurezza dei dati e della privacy degli utenti europei.

Il primo capitolo, verterà quindi sui principali punti di decisione della sentenza *Schrems,* come l'interpretazione della nozione di livello di protezione adeguato, la necessità di stabilire criteri più precisi per la valutazione dell'adeguatezza all'interno della normativa e il riconoscimento della piena indipendenza delle autorità garanti nazionali.

Essa ha avuto notevoli conseguenze sulla disciplina della protezione dati e, in particolare, sulla decisione di adeguatezza della Commissione sull'accordo *Safe Harbor* (decisione 2000/520), la quale è stata dichiarata invalida dalla Corte.

In seguito alla dichiarazione di invalidità da parte della Corte, la Commissione e le autorità Usa hanno dovuto negoziare un nuovo accordo che fosse coerente con le indicazioni dei giudici, al fine di consentire la ripresa degli scambi di dati.

Tale nuovo accordo, denominato *EU-US Privacy Shield* e negoziato all'inizio del 2016, sarà oggetto del capitolo II: si cercherà di valutare se le innovazioni apportate offrono maggiori garanzie per la privacy e la sicurezza dei dati degli utenti e, soprattutto, se gli impegni del governo Usa sulla riforma dei programmi di sorveglianza di massa possono essere sufficienti o se necessitano di maggiori garanzie sostanziali.

Inoltre, si affronteranno alcune questioni legate ad altri strumenti contrattuali utilizzati dalle aziende per trasferire i dati oltre oceano.

Tali strumenti, anch'essi previsti dalla direttiva dati e definiti all'interno di una serie di decisioni della Commissione, sono le *Binding Corporate Rules* (BCR) e le *Standard Contractual Clauses* (SCC).

Si cercherà di capire se essi possono rappresentare un'alternativa valida al meccanismo principale delle decisioni di adeguatezza, sia sotto il profilo della sicurezza e delle garanzie rispetto ai dati personali, sia per quanto riguarda le esigenze delle aziende in termini di costi, tempi di redazione e trasferimenti di dati successivi (cioè quelli effettuati a un soggetto terzo rispetto al contratto).

Infine, il terzo capitolo verterà sull'analisi del nuovo regolamento generale sulla protezione dati 2016/679 che sostituirà, nel maggio 2018, la vecchia direttiva dati 95/46. Esso è destinato a riformare profondamente la protezione dati in Unione europea, innalzando molti degli standard e delle garanzie attuali.

Infatti, accanto a nuovi obblighi per i titolari del trattamento, vi sono nuovi diritti azionabili direttamente dai singoli, come il diritto alla portabilità dei dati e quello all'oblio.

Particolare attenzione sarà dedicata, più specificatamente, al capo V del regolamento inerente il trasferimento internazionale di dati. Ad un prima analisi, esso ricalca, nelle sue linee generali, la precedente disciplina della vecchia direttiva.

Tuttavia, sarà necessario valutare quale impatto possa avere sulle decisioni di adeguatezza precedenti, nonché analizzare le innovazioni inserite per effetto della

sentenza *Schrems*, come i nuovi criteri per la valutazione dell'adeguatezza di un Paese terzo o la ridefinizione delle norme vincolanti di impresa.

Sempre nel corso del terzo capitolo sarà, inoltre, affrontato il tema della compatibilità delle norme sul trasferimento dati con le regole del commercio internazionale dei servizi (accordo GATS), unitamente ad una breve valutazione dei principali suggerimenti indicati dalla dottrina per eventuali future riforme della disciplina, sia sul piano europeo che su quello internazionale.

Capitolo I

Il caso *Schrems* e le sue conseguenze sulla protezione dati in Unione europea

SOMMARIO: 1.1 Premessa; 1.2 Il concetto di privacy: il modello Usa; 1.2.1 Alle origini della privacy negli Stati Uniti; 1.2.2 La disciplina Usa della privacy: la tutela costituzionale e quella ordinaria; 1.3 Il modello europeo: la protezione dati; 1.4 Le origini e la base giuridica dell'accordo *Safe Harbour*; 1.5 Il sistema della decisione *Safe Harbour*: il meccanismo di autoregolamentazione delle imprese statunitensi; 1.6 La sentenza della Corte di giustizia Ue sul caso *Schrems*; 1.6.1 I fatti alla base del rinvio pregiudiziale; 1.6.2 La risposta della Corte di giustizia; 1.6.3 L'invalidità della decisione 520/2000.

1.1 Premessa

Al fine del presente lavoro, prima di analizzare i fatti alla base del caso *Schrems* e la sentenza della Corte di giustizia dell'Unione europea, è utile soffermarsi sull'importanza dell'utilizzo dei dati nel contesto dei rapporti commerciali fra Unione europea e Stati Uniti.

Si può dapprima rilevare come i dati di navigazione degli utenti che utilizzano servizi *web*, piattaforme sociali, motori di ricerca, rappresentano un enorme valore economico e commerciale, e sempre più sono utilizzati nella moderna economia[1].

[1] Si veda, ad esempio, A. Spina*, A Regulatory* Mariage de Figaro*: Risk Regulation, Data Protection, and Data Ethics*, in European Journal of Risk Regulation, 8 (2017), pp. 88-94. L'autore sottolinea come: "the digital economy is fuelled by personal data, quite literally. Its main, and quintessentially defining, commercial applications - such as the Google search engine or a Facebook newsfeed – rely on the collection, use, analysis, and transfer of information concerning individual users. Search engines, apps and digital platforms offer services to users

È esperienza comune e quotidiana quella di svolgere una ricerca utilizzando un motore di ricerca, o di acquistare prodotti e servizi tramite siti internet o applicazioni per *smartphone*.

Già nel 2002 Alessandro Mantelero sottolineava come:

> "nell'attuale momento storico, caratterizzato dalla globalizzazione dell'economia, dalla delocalizzazione delle imprese e dalla diffusione su larga scala delle tecnologie digitali, le informazioni costituiscono la principale delle risorse. I dati servono per migliorare la produzione, per fornire prestazioni, per regolare i rapporti commerciali (…). Il marketing, l'erogazione di servizi e l'informatizzazione di quest'ultimi, assorbono quotidianamente una miriade di dati, ormai indispensabili per il funzionamento di svariate applicazioni tecnologiche"[2].

Ebbene, la maggior parte delle volte tali operazioni avvengono tramite servizi offerti da aziende statunitensi alle quali gli utenti conferiscono grandi quantità di dati personali più o meno consapevolmente, i quali vengono quindi trasferiti oltre oceano e conservati nei *server* dei c.d. colossi del web.

Per molti anni i dati personali, assimilabili a una vera e propria merce, sono stati venduti o scambiati in molti Paesi senza un particolare contesto normativo, in cui le uniche regole erano date dal mercato stesso[3].

---

almost at no cost, the commercial transaction being enabled by the exchange of data. Collection and use of the data are agreed upon by consumers by accepting voluntarily "terms of use".

[2] A. Mantelero, *I flussi transfontalieri di dati personali: l'effetto delle politiche comunitarie*, Contratto e impresa / Europa n. 2, anno settimo, Padova, CEDAM, 2002, p. 1300. Cfr. anche il *Safe Harbor Workbook* del *U.S. Department of Commerce,* consultabile in https://2016.export.gov/safeharbor/eg_main_018238.asp nel quale si dice che "today's information technologies allow information to be collected, compiled, analyzed, and delivered globally more quickly and inexpensively than ever before. Where it was once difficult, time-consuming, and expensive to obtain compile, and analyze information, it is now often available with a few simple clicks of a computer mouse. Increased access to information facilitates personal and political expression as well as commerce, education, and health care. Consumers benefit from the increased access to information. Organizations benefit through reduced costs and client-focused advertising".

[3] *Ibidem*, p.1301.

Tutto ciò fino all'avvento della disciplina europea in materia di trattamento dei dati personali, ossia con l'adozione della direttiva 95/46/CE [4]. Tale disciplina ha rappresentato uno spartiacque non solo all'interno dell'Ue (in cui Paesi membri hanno dovuto adeguare o introdurre *ex novo* una propria normativa interna[5]), ma anche nei rapporti con tutti quei Paesi la cui legislazione in materia di *privacy* e trattamento dati era profondamente diversa.

A questo proposito è utile dare un inquadramento generale al concetto di privacy, alla sua origine e al suo sviluppo nella tradizione statunitense (par. 1.2).

Dopo di che si analizzerà il contrapposto modello europeo incentrato sulla protezione del dato (par. 1.3).

1.2 Il concetto di privacy: il modello Usa

1.2.1 Alle origini della privacy negli Stati Uniti

Le origini del diritto alla privacy devono essere fatte risalire al 1890 quando due celebri giuristi americani pubblicarono un articolo dal titolo *The Right to Privacy*[6].

Esso fornì una prima fondazione giuridica di tale istituto nel quale la privacy venne individuata come un diritto soggettivo fondamentale azionabile davanti a un giudice nei confronti dei privati cittadini[7].

---

[4] Direttiva (CE) 95/46 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, in GUCE L 281 del 23 novembre 1995. Per la verità, all'interno dell'Ue vi erano già alcuni paesi che si erano dotati di una normativa simile fin dagli anni 70', come ad esempio la Germania. Va poi menzionata anche la Convenzione di Strasburgo n. 108 del 1981 sulla protezione degli individui in relazione all'elaborazione automatica dei dati personali, la quale introduceva principi simili all'attuale direttiva.

[5] In Italia la normativa con cui è stata recepita la disciplina della direttiva 95/46 è stata dapprima la Legge n. 675 del 31 dicembre 1996, sulla tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali. Nel 2003 le norme ivi contenute sono state novellate e inserite nel Codice in materia di protezione dei dati personali, di cui al Decreto legislativo 30 giugno 2003 n. 196.

[6] S. Warren, L. Brandeis, *The Right to Privacy*, Harvard Law Review, 1890, vol. V, n. 5.

[7] U. Pagallo*, La tutela della privacy negli Stati Uniti d'America e in Europa: modelli giuridici a confronto*, Milano, Giuffré editore, 2008. Lo stesso autore suggerisce che la nozione era già

Veniva così declinato il *Right to be let alone*, ossia il diritto ad essere lasciati "indisturbati", con l'obiettivo non solo di "impedire che della propria vita privata si offra un ritratto non veritiero ma di impedire che questo ritratto sia in alcun modo eseguito"[8].

Secondo Mantelero, in questa nozione è possibile scorgere l'affermarsi di un:

> "cambiamento culturale di una società che passa da una visione della tutela della persona sostanzialmente fondata sull'intangibilità della proprietà privata a duna nuova concezione incentrata sull'individuo in sé e sulla sua personalità"[9].

Emergevano le esigenze di un nuovo tipo di società, la quale era "incentrata sulla libertà individuale riconosciuta a ciascun uomo, di cui il right to privacy è espressione"[10].

Dovendo procedere a spiegare le argomentazioni alla base delle garanzie da accordare al nuovo diritto in un ordinamento di *common law*, quale quello statunitense, i due autori dovevano affrontare, però, il problema della creazione del diritto senza intervento del legislatore e senza una solida base di precedenti giurisprudenziali al quale fare riferimento[11].

Nel loro saggio, i due avvocati di Boston insistono sul fatto che un ordinamento giuridico è qualcosa che evolve nel tempo, e questo grazie a "nuove esigenze della società" che vengono accompagnate con il progresso tecnologico[12].

Al tempo dei due autori l'esempio che meglio mostra le scoperte della tecnica erano le prime fotografie istantanee, fenomeno che va unito all'enorme crescita della circolazione delle notizie, verificatosi grazie al forte incremento delle vendite dei

---

presente in atre tradizioni o testi normativi, tuttavia quello di Warren e Brandeis è il primo contributo che offre un'esauriente fondazione giuridica dell'istituto. Cfr. anche A. Mantelero, *Il costo della privacy tra valore della persona e ragione di impresa*, Milano, Giuffré editore, 2007, p. 2, in cui si fa riferimento a come il giudice T. Cooley aveva già anticipato il *Right to be let alone* come diritto della persona nel suo saggio *A treatise on the Law of Torts*, Chicago, 1888.

[8] Cfr. S. Warren, L. Brandeis, op. cit., p. 111.

[9] Cfr. A Mantelero, op. cit. (2007), p. 3.

[10] *Ibidem*.

[11] Cfr. U. Pagallo, op. cit., p. 5.

[12] Cfr. S Warren, L. Brandeis, op. cit., p. 45.

giornali[13]: la circolazione abusiva di immagini personali, sfruttabili per la prima volta su larga scala grazie, appunto, alla stampa, era destinata a produrre effetti negativi a cui l'ordinamento giuridico doveva porre rimedio tramite adeguati mezzi di tutela[14].

I primi casi di applicazione del nuovo istituto nell'ordinamento Usa si ebbero all'inizio del 900'. Fu la Corte dello Stato della Georgia ad asserire che "il diritto alla privacy nelle materie puramente private è per ciò derivato dal diritto naturale", riconoscendo così per la prima volta la sua tutela[15].

La privacy è stata, quindi, dapprima interpretata come "non intrusione" o "esclusione" degli altri dalla propria vita.

Nel primo senso come "diritto dell'individuo di essere libero da intrusioni pubbliche non autorizzate"[16], e quindi come strumento per garantire un'ampia tutela […] rispetto ai comportamenti intrusivi posti in essere dai pubblici poteri"[17].

La seconda accezione, invece, è intesa come necessità di una persona di rendersi inaccessibile agli altri, cioè un diritto "di escludere gli altri dalla nostra vita, e di vivere conseguentemente appartati, in santa pace e tranquillità"[18].

A partire dal caso *Pavesich*, prima citato, è stata questa la chiave interpretativa usata dai giudici nell'applicare la nozione di privacy; essa è stata comunque affiancata ad ulteriori obiettivi di tutela, così che sono state individuate altre sfaccettature del concetto di privacy, sempre nel contesto giurisprudenziale, come la *political privacy*, l'*associational privacy*, la *privacy of counsel*, e la *privacy* connessa alla libertà sessuale e di aborto[19].

---

[13] Si registra che tra il 1850 e il 1890 la vendita di giornali negli Stati Uniti incrementò di circa il 1000%; cfr. a tale proposito A. Mantelero, p. 11.
[14] Cfr. U. Pagallo, op. cit., p. 7.
[15] Caso *Pavesich v. New England Life Insurance Co*., 50 S.E 68 (Ga. 1905), citato in U. Pagallo, p.8.
[16] Cfr. U. Pagallo, op. cit., p. 40, il quale ricorda che tale interpretazione, data anche da William Brennan, giudice della Corte suprema nel caso *Eisenstadt v. Baird* del 1972, rischia "di perdere di vista il fatto che la privacy è ciò che rende possibile l'esercizio di una data libertà, non coincidendo, però, con la libertà stessa o con la condizione, o contenuto, con cui volta per volta si identifica l'istituto".
[17] Cfr. A. Mantelero, op. cit., p. 7.
[18] Cfr. U. Pagallo, op. cit., pp. 40-41.
[19] Cfr. A. Mantelero, op. cit., pp. 7-8.

A sostegno di tale evoluzione è utile portare l'esempio di William Prosser, il quale, nel 1960, compiendo una ricognizione della giurisprudenza delle Corti Usa, ha catalogato oltre trecento fattispecie diverse in tema di responsabilità civile correlata alla privacy[20].

Nel corso del tempo la nozione di privacy è stata, quindi, ampliata e ne è stato sviluppato il contenuto iniziale, secondo l'intento originario di Warren e Brandeis[21].

Nonostante la moltitudine di concetti che si sono accumulati nel tempo sotto il nome *privacy* nel *common law* statunitense – derivanti dalla giurisprudenza della Corte suprema e da quella dei singoli Stati - è comunque possibile delineare un modello americano di privacy[22].

Nel presente lavoro si cercherà, quindi, di trattare, a linee generali, la disciplina della tutela della privacy nell'ordinamento Usa.

1.2.2 La disciplina Usa della privacy: la tutela costituzionale e quella ordinaria

Il modello statunitense della protezione della privacy si presenta come un sistema di tipo "settoriale", nel senso che non è presente un quadro normativo generale a carattere federale[23].

Tuttavia, pur mancando una legislazione federale generale, la tutela della privacy è stata comunque accordata dal diritto costituzionale per opera della giurisprudenza della Corte suprema che ha interpretato, nel corso degli anni, la Costituzione federale[24].

---

[20] Si veda W. Prosser, *Privacy*, in California Law Review, 1960, 48, citato in U. Pagallo, op. cit., p. 62.

[21] Cfr. U. Pagallo, op. cit., p. 67.

[22] Così U. Pagallo, op. cit., p. 68, muovendo dalle considerazioni di C. Albernathy, *Defining privacy: the power of culture in the digital age*, nella relazione presentata al convegno sulla Privacy digitale organizzata dall'università di Torino il 18-19 aprile 2005.

[23] Cfr. U. Pagallo, op. cit., p. 61.

[24] A questo proposito è utile ricordare in che modo opera la giustizia costituzionale nel sistema federale Usa. Si tratta di un controllo costituzionale di tipo diffuso delle legge ordinarie affidato ai giudici ordinari: essi, quindi, sono tenuti a valutare la conformità di una legge ordinaria alla Costituzione, eventualmente disapplicando la disposizione contrastante con essa. Tale decisione

In particolare, pur mancando nella costituzione un esplicito riferimento alla *privacy*, la Corte di Washington, a partire dal caso *Griswold v. Connecticut* del 1965[25], ha interpretato il primo e il quarto emendamento[26], riconoscendo in essi la *privacy* come oggetto di tutela in rapporto sia alla vita pubblica delle persone sia alla loro sfera privata e familiare[27].

È stato sottolineato come una delle particolarità della tutela costituzionale della privacy negli Usa è data dal fatto che essa:

> "riconosce una 'zona franca' per la quale è proibito l'intervento del governo federale negli affari personali degli individui, là dove spetta invece agli stati federati di garantire, eventualmente, tramite azioni 'positive' o 'affermative', un maggiore sfera di tutela della privacy rispetto al *minimo* previsto costituzionalmente"[28].

Per quanto riguarda, invece, la tutela ordinaria della privacy, l'ordinamento Usa prevede una disciplina che è possibile suddividere in due parti.

Da un lato si ha la legislazione federale, dall'altro quella derivante dai singoli stati federati.

Sul piano federale la tutela è accordata principalmente al piano dei rapporti fra governo e individui; la legge di riferimento è il *Privacy Act* del 1974[29].

---

ha valore solo nei confronti delle parti in giudizio. La coerenza del sistema è affidata all'organo di vertice del sistema giudiziario, la Corte suprema, le cui decisioni, in base al principio dello *stare decisis*, vincolano tutti i giudici. Si veda, in proposito, E. Palici di Suni, *Tre modelli di giustizia costituzionale*, in Rivista AIC n. 1/2016, reperibile in: http://www.rivistaaic.it/tre-modelli-di-giustizia-costituzionale.html

[25] Caso *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[26] Il primo emendamento stabilisce che "Il Congresso non potrà fare alcuna legge […]che limiti la libertà di parola o di stampa"; il quarto stabilisce, invece, "il diritto dei cittadini ad essere assicurati nelle loro persone, case, carte ed effetti contro perquisizioni e sequestri non ragionevoli, non potrà essere violato, e non potranno essere emessi mandati se non su motivi probabili, sostenuti da giuramenti o solenni affermazioni e con una dettagliata descrizione del luogo da perquisire e delle persone o cose da prendere in custodia".

[27] Cfr. U. Pagallo, op. cit., p. 61.

[28] *Idem,* p. 69.

[29] The Privacy Act of 1974, 5 U.S.C. § 552a.