Alma Mater Studiorum – Università di Bologna

DOTTORATO DI RICERCA IN

DIRITTO DELL'UNIONE EUROPEA

Ciclo XXV

Settore Concorsuale di afferenza: 12/E1

Settore Scientifico disciplinare: IUS/14

TITOLO TESI

LA DIMENSIONE ESTERNA DELLA TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA

Presentata da: **Luca Favero**

Coordinatore Dottorato **Relatore**

Prof.ssa Lucia Serena Rossi **Prof.ssa Lucia Serena Rossi**

Esame finale anno 2013

INDICE

PARTE SECONDA

LA VICENDA SWIFT E L'ACCORDO TFTP II

PARTE TERZA

IL CONTENZIOSO USA-UE NELL'AMBITO DELLA VICENDA PNR

PARTE QUARTA

Bibliografia

INTRODUZIONE

Questa tesi di dottorato ha per oggetto la dimensione esterna della tutela dei dati personali nel diritto dell'Unione Europea, ossia l'analisi dei meccanismi attraverso i quali il diritto dell'Unione assicura ai dati personali che vengono trasferiti verso Paesi terzi un elevato livello di protezione. La tesi si propone, quindi, di evidenziare i risultati conseguiti alla luce di quella che si dimostra sempre di più essere una vera e propria "politica estera legislativa" dell'Unione Europea in questa materia.

Particolare attenzione verrà dedicata alle relazioni tra Stati Uniti ed Unione Europea e ciò alla luce del moderno contenzioso tra le due sponde dell'Atlantico sul versante della tutela dei dati personali. Negli ultimi anni, infatti, il fenomeno del trasferimento internazionale dei dati personali non è più legato esclusivamente a ragioni di carattere commerciale ma, sempre più spesso, risulta connesso ad esigenze di protezione della sicurezza pubblica[1]. Invero, la condivisione tra le autorità di polizia di Paesi differenti dei dati personali relativi ai propri cittadini è divenuta un elemento essenziale nel quadro della cooperazione internazionale contro il terrorismo ed il crimine organizzato internazionale[2].

Come si vedrà, dunque, il diritto dell'Unione Europea viene, così, costantemente confrontato con l'esigenza di bilanciare gli imperativi della sicurezza pubblica con la tutela del diritto fondamentale dell'individuo alla propria privacy.

Il presente elaborato è suddiviso in quattro capitoli.

Il primo e il secondo capitolo sono strutturati in modo tale da offrire una comparazione tra il diritto federale degli Stati Uniti d'America e quello dell'Unione Europea in materia di tutela dei dati personali. Tale comparazione è diretta a porre in evidenza le differenze, anche di carattere storico e culturale, nella concezione di tutela dei dati personali da parte dei due ordinamenti giuridici e le conseguenze che tale diversa concezione comporta sulle rispettive legislazioni e sulla giurisprudenza.

Il primo capitolo contiene, dunque, l'analisi dei casi giurisprudenziali più importanti decisi dalla Corte Suprema Federale oltre che la descrizione dell'approccio settoriale tipico della legislazione degli Stati Uniti.

Il secondo capitolo, invece, è dedicato all'esame della giurisprudenza e della legislazione primaria europea, segnatamente della Direttiva 95/46/CE.

[1] Marco Botta, Mario Viola De Azevedo Cunha "*La Protezione dei dati personali nelle relazioni tra USA e UE, le negoziazioni sul trasferimento dei PNR*", in Diritto dell'Informazione e dell'Informatica, 2010, 2, p. 315
[2] Idem

Il terzo capitolo contiene un esame critico del progetto di riforma della Direttiva 95/46/CE varato nel gennaio del 2012, e delle conseguenze che esso avrà sulla disciplina del trasferimento all'estero di dati personali.

Il quarto capitolo, infine, si concentra su di un'analisi approfondita delle disposizioni della Direttiva 95/46/CE che regolano i trasferimenti di dati personali all'estero, tra cui le decisioni sull'adeguatezza della Commissione ed il regime delle deroghe al principio del livello adeguato di protezione.

Inoltre, in tale sede vengono illustrati anche le vicende che hanno interessato i principali accordi conclusi tra l'Unione Europea e gli Stati Uniti in materia di trasferimento e condivisione dei dati personali.

Infine, in sede di conclusioni verranno illustrati i risultati raggiunti dalla dimensione esterna della tutela dei dati personali nel diritto dell'Unione Europea

CAPITOLO I

LA TUTELA DEI DATI PERSONALI NEL DIRITTO FEDERALE DEGLI STATI UNITI D'AMERICA

1. Due modi di concepire la privacy: un confronto tra la legislazione americana e quella europea in materia di protezione della riservatezza e dei dati personali.

Come si vedrà in prosieguo, Stati Uniti e Unione Europea hanno adottato due approcci legislativi molto distinti e, per molti versi, inconciliabili nella tutela della privacy e dei dati personali. L'Unione Europea ambisce, infatti, a restringere ed a disciplinare rigorosamente i casi di trattamento dei dati personali e ad impedire che questi ultimi siano utilizzati per finalità diverse da quelle dichiarate. La legislazione degli Stati Uniti, dal canto suo, consente più ampie possibilità di raccolta e di registrazione dei dati e, quindi, una maggiore penetrazione nella privacy degli individui[3].

Inoltre, mentre l'Unione Europea ha adottato in materia una legge generale, ossia la Direttiva 95/46/CE, che copre tendenzialmente l'intera gamma delle possibili modalità di trattamento dei dati personali, gli Stati Uniti si sono dotati di una legislazione frammentaria, che non ha portata generale, bensì disciplina uno ad uno singoli e specifici ambiti di trattamento dei dati[4].

Questa differenza di fondo nella concezione della protezione della privacy, da parte degli Stati Uniti e dell'Unione Europea, si pone all'origine del contenzioso internazionale USA-UE relativo al trasferimento dei dati personali, come testimoniato dalle vicende Swift e PNR di cui si parlerà più avanti in questa tesi.

Non è certamente l'obiettivo di questo lavoro quello di presentare un'analisi dettagliata della legislazione americana in materia di protezione dei dati personali. Negli USA, infatti, accanto all'ordinamento giuridico federale esistono tanti singoli ordinamenti separati quanti sono i singoli Stati che li compongono[5].

---

[3] Marsha Cope Huie; Stephen F. Laribee; Stephen D. Hogan, *The right to privacy in personal data: the EU prods the US and controversy continues*, in Tulsa Journal of Comparative and International Law, Spring 2002, Vol. 9 Issue 2, p391-469, 79p

[4] Matthew R. Van Wasshnova, "*Data protection conflicts between the United States and the European Union in the war on terror: lessons learned from the existing system of financial information exchange*", in Case Western Journal of International Law, 2007/2008, Vol. 39 Issue 1/2, p827-865, 39p

[5] Ugo Mattei, *Il Modello di Common Law*, Torino 2004 p. 250.

A ben vedere, inoltre, una analisi relativa alla legislazione dei singoli stati non avrebbe alcuna rilevanza ai fini della presente ricerca, dal momento in cui gli accordi con l'Unione Europea sui trasferimenti di dati sono stati conclusi dal Governo federale.

Tuttavia, nulla di quanto ora detto impedisce di fare delle considerazioni generali in merito a come viene concepita la tutela della privacy nel diritto federale statunitense, ragionando sia in termini di *case law* che di leggi federali, senza ovviamente omettere un cenno alla questione della *self regulation*. Tale premessa è infatti indispensabile per comprendere le ragioni che stanno alla base del diverso approccio alla privacy da parte dei due ordinamenti e che, di conseguenza, si pongono a fondamento del confronto transatlantico relativo agli accordi sul trasferimento dei dati personali.

2. La tutela della Privacy nel diritto federale degli Stati Uniti d'America. Premessa

Negli Stati Uniti d'America la nozione di "*privacy*" è molto ampia e suscettibile di ricomprendere situazioni giuridiche assai eterogenee. Poiché negli USA non esiste una definizione giuridica di privacy universalmente accettata, in tale concezione rientrano situazioni che vanno dal diritto di una donna ad interrompere la gravidanza a quello degli individui di fare ricorso alla contraccezione senza alcuna ingerenza da parte delle autorità statali[6].

Inoltre, come già accennato, la legislazione americana in materia di privacy si distingue per il suo carattere frammentario, circostanza che ha indotto la stessa dottrina d'oltreoceano a parlare di "*patchwork quilt legislation*"[7], con ciò alludendo ad una regolamentazione a macchia di leopardo.

Il regime di tutela federale della privacy negli USA non si fonda, infatti, su di una legge generale bensì, essenzialmente, su pronunce giurisprudenziali, su specifiche leggi federali nonché sulla *self regulation* da parte degli enti e delle industrie[8]. Come si vedrà più avanti, inoltre, è pure registrabile una discrepanza tra il livello di tut2ela nel settore pubblico e quello

[6] Dorothee Heisenberg, "*Negotiating Privacy : the European Union, the United States, and personal data protection",* Londra 2005
[7] Marsha Cope Huie; Stephen F. Laribee; Stephen D. Hogan, nota 3
[8] *Idem*

vigente nel settore privato, ambito in cui il Congresso americano è tradizionalmente più restio ad intervenire[9].

Tutto questo non deve, ovviamente, indurre a concludere che negli Stati Uniti d'America la tutela della privacy sia un'esigenza poco avvertita[10]. Al contrario, per il *common law* americano il diritto alla privacy riveste un'indubbia importanza[11]. Non soltanto vi è, infatti, una vasta letteratura giuridica in materia ma anche numerosi principi alla base della stessa legislazione europea e delle linee guida internazionali sono tributari dell'esperienza statunitense[12].

Ciò premesso, è anche vero che, mentre in Europa la privacy gode dello *status* di diritto fondamentale stante la sua inclusione nella Carta dei Diritti Fondamentali dell'Unione Europea e nel Trattato di Lisbona, negli Stati Uniti d'America essa non rientra in quanto tale tra i diritti costituzionalmente garantiti. Né la Costituzione Federale né il cd. "*Bill of Rights*" contemplano esplicitamente uno specifico diritto alla riservatezza.

Soltanto il *Fourth Amendment* contiene una norma che si avvicina a tale concetto laddove prevede che *"the right of the people to be secure in their persons, houses papers, and effects, against unreasonable searches and seizures, shall not be violated".* E' evidente però che la protezione offerta da detta disposizione è stata pensata con riferimento alle ipotesi di ingerenza da parte dei pubblici poteri a difesa del diritto di proprietà e di libertà individuale.

In realtà fu soltanto nel 1890, a seguito della pubblicazione della celebre *law review* di Samuel Warren e Louis Brandeis[13], che la dottrina americana, preoccupata dalla recente comparsa della fotografia nonché della spregiudicatezza della stampa sensazionalista, iniziò ad interrogarsi in merito all'esistenza di un generale diritto dell'individuo "*to be let alone*"[14].

In particolare, in tale *law review* i due illustri giuristi statunitensi muovevano dal carattere vivente del *common law* il quale, nella sua "*eterna giovinezza*" si evolve affermando l'esistenza di nuovi diritti, rispondendo così alle rinnovate esigenze della società dettate dai costanti cambiamenti politici economici e sociali[15].

Per questa ragione, dinnanzi all'invasione dei "*sacri recinti della vita privata e domestica*" ed alla circolazione indiscriminata di ritratti non autorizzati di persone, per la prima volta venne teorizzata la possibilità di estendere alla tutela della riservatezza la

[9] Laura B. Pincus, Clayton Trotter, *The disparity between public and private sector employee privacy protection: a call for legitimate privacy rights for private sector workers*, in American Business Law Journal 1995
[10] Dorothee Heisenberg, nota 6
[11] Idem
[12] ibidem
[13] S. Warren e L. Brandeis, "*The right to privacy*", in *Harvard Law Review*, 4 HAv. L. REv. 193 (1890) H
[14] In realtà tale nozione era già presente in Thomas M. Cooley , *"Law of Torts"* edito per la prima volta nel 1880
[15] V. amplius *Olmstead vs. United States* 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting)

protezione accordata dal *common law* americano alla proprietà privata, all'onore ed alle obbligazioni contrattuali[16].

Successivamente, negli anni '60, allorquando la formulazione di Warren e Brandeis iniziava ad apparire eccessivamente vaga, le teorie del professor William Prosser contribuirono a dare vita ad una vera e propria *privacy torts law*[17]. Prosser individuava, infatti, sulla base di un'analisi delle pronunce delle corti statunitensi quattro componenti essenziali del diritto alla privacy che includevano

1. l'invasione nella riservatezza di un individuo
2. il divieto di pubblicare fatti privati ed imbarazzanti
3. il divieto di pubblicare fatti che pongano l'individuo in una falsa luce
4. l'appropriazione non autorizzata del nome o delle sembianze di altro individuo per il proprio vantaggio personale[18]

Tali principi sono alla base del moderno *tort law* statunitense in materia di privacy e il concetto di "*invasion of privacy*" è tutt'oggi comunemente utilizzato nelle corti americane[19].

Nel suo articolo Prosser traeva spunto dalla significatività del caso *Yoeckel vs. Samonig*[20] deciso dalle corti del Wisconsin[21]. La causa verteva sulla condotta del proprietario di una taverna che, entrato nella toilette delle donne, aveva fotografato una cliente per poi mostrarne la foto agli altri frequentatori del locale. In quell'epoca, tuttavia, la legislazione del Wisconsin aveva rigettato l'idea di un diritto alla privacy, sicché la parte lesa, Norma Yoeckel, non poté richiedere il ristoro del pregiudizio subito a fronte della divulgazione, oltraggiosa e contro la sua volontà, di dati privati ed intimi[22].

Sul versante della giurisprudenza, invece, si registrano sin dal 1905 diverse pronunce, soprattutto da parte di corti statali, in merito al riconoscimento di un diritto d'azione per l'invasione della privacy. Tuttavia, l'estensione specifica di questo diritto così come riconosciuto in via pretoria rimaneva poco chiara, mancando ancora una teoria generale ed essendo rilevato di volta in volta secondo un approccio casistico.

In ogni caso, come si vedrà, sebbene le pronunce in materia di privacy delle corti statali iniziarono ad evolversi in epoca relativamente recente, esse furono ben presto eclissate

[16] S. Warren e L. Brandeis, cit sub nota 13
[17] William Prosser, *Privacy*, California Law Review Vol. 48 August 1960 No. 3
[18] idem
[19] Dorothee Heisenberg cit. sub nota 6
[20] Yoeckel v. Samonig, 272 Wis. 430, 75 N.W.2d 925 (1956),
[21] Osserva, in particolare, William Prosser che "..t*he last decision... involved a particularly outrageous invasion, when the defendant intruded into a ladies' rest room, photographed the plaintiff there, and exhibited the picture to patrons in a restaurant.The court bowed to the fact that a bill providing for the right of privacy had failed to pass in the last legislature. The case is nevertheless an atrocity".*
[22] William Prosser, nota 17

dall'evoluzione della giurisprudenza della Corte Suprema Federale degli Stati Uniti d'America.[23]

3. Considerazioni sulla giurisprudenza della Corte Suprema USA in materia di tutela della privacy

La Corte Suprema federale statunitense non ha paragoni istituzionali altrove, né nella tradizione di *civil law*, né in quella di *common law*. Secondo un eminente autore americano "*la Corte Suprema è oggi il corrispondente della monarchia inglese. Ma a differenza della Regina sul trono, essa ha vero potere*"[24].

La sua giurisdizione è scandita dal terzo articolo della Costituzione nonché dalle sezioni 1251 e ss. del *US Code*. Essa è divisa tra una giurisdizione originaria, in materia di conflitto fra i diversi Stati[25], ed una giurisdizione d'appello. Quest'ultima si esercita tanto nei confronti delle Corti Federali inferiori[26] quanto nei confronti delle Corti statali di ultima istanza nelle ipotesi in cui sia coinvolta una *federal question*[27].

Peraltro, soltanto nei confronti delle Corti federali inferiori essa ha l'ultima parola, potendo rendere un giudizio finale[28]. Viceversa, nei confronti delle Corti statali di ultima istanza essa decide autoritativamente sulla sola questione federale, rimandando il giudizio alla

---

[23] Shaman, Jeffrey M., *The right of privacy in state constitutional law*, Rutgers Law Journal, Summer 2006, Vol. 37 Issue 4, p971-1085, 115p

[24] Mason, *Judicial Activism: Old and New*, in 55 Va. Law Review 411 (1969)

[25] 28 USC § 1251 - *Original jurisdiction:*

"(a)The Supreme Court shall have original and exclusive jurisdiction of all controversies between two or more States.
(b)The Supreme Court shall have original but not exclusive jurisdiction of:

(1)All actions or proceedings to which ambassadors, other public ministers, consuls, or vice consuls of foreign states are parties;

(2)All controversies between the United States and a State;

(3)All actions or proceedings by a State against the citizens of another State or against aliens".

[26] 28 USC § 1253 - *Direct appeals from decisions of three-judge courts: " Except as otherwise provided by law, any party may appeal to the Supreme Court from an order granting or denying, after notice and hearing, an interlocutory or permanent injunction in any civil action, suit or proceeding required by any Act of Congress to be heard and determined by a district court of three judges".*

[27] 28 USC § 1257 – "*State courts; certiorari*

(a)Final judgments or decrees rendered by the highest court of a State in which a decision could be had, may be reviewed by the Supreme Court by writ of certiorari where the validity of a treaty or statute of the United States is drawn in question or where the validity of a statute of any State is drawn in question on the ground of its being repugnant to the Constitution, treaties, or laws of the United States, or where any title, right, privilege, or immunity is specially set up or claimed under the Constitution or the treaties or statutes of, or any commission held or authority exercised under, the United States.

(b)For the purposes of this section, the term "highest court of a State" includes the District of Columbia Court of Appeals".

[28] Ugo Mattei, nota 5

corte statale per ulteriori procedimenti non incompatibili con la sua decisione[29]. Inoltre la Corte Suprema seleziona la casistica di cui occuparsi mediante il cd. *writ of certiorari*[30].

Il ruolo della Corte Suprema Federale di guardiana della Costituzione è stato affermato per la prima volta nel celebre caso Marbury vs. Madison[31] del 1803. In tale caso, avente ad oggetto la costituzionalità della Sezione 13 del Judicial Code del 1789, la Corte Suprema ha introdotto la nozione di "*judicial review*", affermando per la prima volta il concetto di incostituzionalità di una legge statale. Infatti, secondo il ragionamento seguito dalla Corte Suprema, considerato che le prerogative del potere Legislativo sono definite e limitate, i Padri Fondatori hanno previsto una Costituzione scritta affinché tali limiti non vengano elusi o ignorati [32]. Conseguentemente, un atto normativo contrario alla Costituzione, che costituisce la legge fondamentale della Nazione, deve ritenersi nullo e privo di efficacia. In caso di contrasto tra la Costituzione e una legge federale, dunque, i giudici devono applicare la Costituzione, ignorando la legge federale[33].

Di pari passo, giova evidenziare come il controllo della costituzionalità delle leggi negli USA sia di carattere diffuso anziché, come ad esempio in Italia, di tipo accentrato[34]. Ciò implica che il potere di disapplicare una legge in quanto incostituzionale non è una prerogativa esclusiva della Suprema Corte, bensì un dovere che compete a tutti i giudici americani[35].

Ad avviso di chi scrive, tutto ciò ha una notevole influenza sulla mentalità giuridica degli operatori del diritto statunitensi i quali, probabilmente in maniera molto più accentuata rispetto ai propri colleghi europei, risultano inclini a valutare con maggiore attenzione la dimensione costituzionale di qualsiasi questione giuridica. E' sempre convinzione di chi scrive, tuttavia, che questa diversità tra i poteri dei giudici americani e quelli europei risulta oggi meno profonda rispetto al passato grazie all'avvento del diritto europeo e del relativo primato sul diritto interno, che consente in maniera del tutto simile a quanto avviene negli USA, la disapplicazione del diritto nazionale in contrasto con la legislazione europea.

Il caso Marbury vs. Madison rappresenta una pietra miliare nella giurisprudenza costituzionale americana e il *judicial review* della legislazione statale e federale costituisce ancora oggi l'aspetto più caratteristico e controverso del common law americano. Esso,

[29] Idem
[30] Shaman, Jeffrey M, nota 23
[31] Marbury v. Madison, 5 U.S. (1 Cranch) 137 (1803)
[32] Idem, Page 5 U. S. 176
[33] Idem 5 U. S. 177
[34] Ugo Mattei, nota 5 p. 320
[35] Idem

infatti, ha reso il potere giudiziario, il potere più forte nel sistema federale statunitense, tanto che tra gli operatori del diritto americano è invalsa la convinzione per cui la Costituzione afferma sostanzialmente ciò che la Suprema Corte Federale vuole che essa dica[36].

Allo stesso modo occorre segnalare che l'attivismo della Corte Suprema attraverso lo strumento del *judicial review* ha comunque destato non poche perplessità in seno alla dottrina statunitense se non altro per la discrezionalità, da parte della Corte, nel delineare fattispecie il cui ancoraggio al testo normativo scritto risulta sempre più remoto, tanto da portare a considerare le sue sentenze come una fonte normativa "*sui generis*" di diritto «a base giurisprudenziale». Invero, passo dopo passo, la Corte Suprema Americana ha conquistato un sempre maggiore ed oggi esclusivo diritto di determinare il significato della Costituzione federale. Pertanto, a partire dal caso Marbury vs. Madison in cui veniva proclamato sommessamente il dovere del potere giudiziario di dire ciò che la legge é, si è passati al caso *Cooper vs. Aaron*[37] del 1958 in cui la Corte Suprema, all'unanimità ha proclamato la propria supremazia "*nell'esposizione del diritto della Costituzione*". Successivamente nel caso *Boumediene vs. Bush*[38] la Corte ha fatto un passo ulteriore, superando lo sforzo del Congresso di limitare la sua giurisdizione ignorando le restrizioni alla sua giurisdizione previsti in una serie di leggi in materia di nemici combattenti detenuti.

Ciò premesso, il *leading case* in materia di tutela della privacy nella giurisprudenza della Corte Suprema è senz'altro rappresentato dal caso *Griswold vs. Connecticut* del 1965[39]. Questo caso verteva sulla costituzionalità di una legge statale che proibiva l'utilizzo di tecniche contraccettive quale sistema di controllo delle nascite, nonché l'attività di assistenza medica nel campo della contraccezione.

A parere della Suprema Corte tale legge, nel proibire *tout court* l'uso di contraccettivi anziché regolarne la produzione o la vendita, attuava le proprie finalità attraverso un impatto eccessivo ed irragionevole sulle relazioni matrimoniali, le quali si collocavano all'interno di un'area di privacy creata da diverse garanzie costituzionali le cui origini dovevano ritenersi addirittura più antiche dello stesso *Bill of Rights*.

Una tale legge, pertanto, non appariva conforme al principio per cui gli obiettivi di controllo e di prevenzione da parte dello Stato non possono esplicarsi attraverso modalità tali da invadere l'area delle libertà fondamentali. Ritenendo, quindi, che una coppia sposata

[36] Malcolm, Joyce Lee Joyce Lee Malcolm, "Whatever the Judges Say It Is? The Founders and Judicial Review", The Journal of Law & Politics 26 no1 1-37 Fall 2010
[37] Cooper vs. Aaron, 358 U.S. 1 (1958)
[38] Boumediene v. Bush, 553 U.S. 723 (2008),
[39] *Griswold vs. Connecticut*, 381 U.S. 479, 484 (1965)

avesse tutto il diritto di ricorrere alla contraccezione, la Corte Suprema dichiarò la legge dello stato del Connecticut incostituzionale[40].

Ma al di là degli specifici fatti di causa, la sentenza *Griswold* viene ricordata nella letteratura statunitense in ragione del fatto che con essa la Corte Suprema affermava per la prima volta l'esistenza di un implicito diritto alla privacy all'interno della Costituzione americana[41]. Osservava, infatti, la Corte che "*specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance"* e che *"various guarantees create zones of privacy".* In altre parole la sentenza *Griswold* enunciava la cd. "teoria della penombra", in virtù della quale varie disposizioni del *Bill of Rights* conterrebbero delle aree in cui potrebbe agevolmente collocarsi la tutela di singoli aspetti del diritto alla privacy[42].

Infatti, secondo la Corte *"(...) various guarantees create zones of privacy. The right of association (...) in the penumbra of the First Amendment is one (...). The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment (....) "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures". The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people (...)."*[43]

Con la sentenza *Griswold* veniva, in definitiva, affermato il concetto per cui ciascuna delle disposizioni del *Bill of Rights* ivi considerate conterrebbe un aspetto della tutela della privacy individuale, ovvero un inedito "*privacy right against the State's need for safety and security*"[44].

Sette anni dopo, nel caso *Eisenstadt vs. Baird* la Suprema Corte applicava la teoria della penombra alla *Equal Protection Clause* del quattordicesimo emendamento, così estendendo il diritto all'uso dei contraccettivi anche agli individui non sposati, e ciò sul

[40] *Griswold vs. Connecticut, cit. sub nota 30 ""*(...)w*ould we allow the police to search the sacred precincts of marital bedrooms for telltale signs of the use of contraceptives? The very idea is repulsive to the notions of privacy surrounding the marriage relationship(…)."*
[41] Honorable Major B. Harding, Mark J. Criser e Michael R. Ufferman, "*Right to be let alone? Has the adoption of article I, section 23 in the Florida Constitution, which explicitly provides for a State right of privacy, resulted in greater privacy protection for Florida citizens?*" in Notre Dame Journal of Law, Ethic and Public Policy, 14 n. 2 945-1009 2000.
[42] Shaman, Jeffrey M, nota 23.
[43] *Griswold vs. Connecticut, cit.* sub nota 39
[44] *Idem*

presupposto che la privacy deve intendersi come uno specifico diritto dell'individuo[45]. Nel caso *Loving vs. Virginia*, invece, la Suprema Corte dichiarava incostituzionale una legge che proibiva i matrimoni misti per contrasto con la *due process clause* del quattordicesimo emendamento, affermando che la libertà di sposarsi è un vitale interesse personale protetto dalla Costituzione[46].

Successivamente, nel caso *Roe vs. Wade* del 1973[47], la Suprema Corte mutò parzialmente il proprio orientamento, precisando ulteriormente il concetto di "*zone of privacy*" già affermato in *Griswold*. Tale ulteriore caso, sollevato da una donna in stato interessante, verteva sulla presunta incostituzionalità di una legge del Texas che vietava l'aborto in ogni fase della gravidanza salva l'ipotesi in cui esso fosse necessario per salvare la vita della madre.

Nella sua decisione la Corte Suprema ritenne che il diritto di una madre ad interrompere la gravidanza mediante aborto fosse protetto dal diritto costituzionale alla privacy. Tuttavia, tale diritto non era assoluto, in quanto doveva essere bilanciato con altri importanti interessi legislativi dello Stato. Ma poiché esso rivestiva comunque carattere fondamentale, la sua limitazione mediante legge poteva essere giustificata soltanto da un interesse preminente dello Stato. Applicando tali principi alla legge del Texas la Corte Suprema concluse per la sua incostituzionalità.

In particolare nella sentenza *Roe* , contrariamente a quanto ritenuto in *Griswold*, la Corte affermò che il diritto alla privacy trovava sicuro fondamento nel quattordicesimo emendamento. Accantonata, dunque, la teoria della penombra, la Corte stabiliva altresì che soltanto i diritti fondamentali della persona o quelli che sono impliciti nella nozione di libertà individuale sono protetti dalla privacy. Procedeva, dunque, a stillare un elenco tassativo di questi diritti individuandoli nel matrimonio, nella procreazione, nella contraccezione, nelle relazioni familiari e nella crescita ed educazione dei figli.

In altre parole, dalla giurisprudenza della Corte Suprema ora esaminata parrebbe evincersi che la privacy, lungi dal configurare un autonomo diritto degli individui, assumerebbe carattere strumentale solamente in relazione alla protezione dei diritti fondamentali dell'individuo individuati dalla Corte stessa o che verrebbe comunque in rilievo soltanto in funzione di quelli.

---

[45] *Eisenstadt vs. Baird* 405 U.S. 438-453 (1972) *"If the right of privacy means anything, it is the right of the individual, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child*".

[46] *Loving vs. Virginia* 388 U.S. 1 (1967)

[47] *Roe vs. Wade*, 410 U.S. 113 (1973)

A dimostrazione di quanto ora detto, dopo la sentenza *Roe* vi sono stati numerosi tentativi di estendere la tutela della privacy al di là delle ipotesi ora richiamate. Salvo rare eccezioni, tuttavia, quali ad esempio l'invalidazione di leggi che vietavano la vendita di contraccettivi a minorenni[48], la Corte si è sempre rifiutata di allargare la portata della giurisprudenza *Roe*. In questo senso la Corte, inizialmente, non ha ritenuto di estendere la tutela della privacy al diritto di intrattenere rapporti omosessuali[49], salvo poi correggere parzialmente il tiro estendendo detta tutela anche alle attività sessuali individuali in generale[50].

Successivamente, nel caso *Lawrence vs. Texas*[51], la Corte Suprema, non senza imbarazzo per il metro di giustizia impiegato quindici anni orsono, ribaltava la giurisprudenza *Hardwick* dichiarando incostituzionale una legge del Texas che qualificava i rapporti omosessuali tra adulti consenzienti come reato.

Infine, nel caso Whalen vs. Roe la Corte ha, altresì, negato l'estensione del diritto costituzionale alla privacy all'attività di raccolta dei dati personali da parte del Governo[52].

Alla luce di quanto finora detto si noterà come la Corte Suprema, dopo un periodo di iniziale attivismo, ha iniziato a mostrarsi riluttante verso ulteriori approfondimenti del diritto alla privacy i cui contorni, salvo qualche significativa eccezioni, sembrano essere stati definitivamente scolpiti dalla giurisprudenza *Roe*.

In ogni caso, essa ha chiarito un punto fondamentale. Nel caso *Katz vs. United States*[53], infatti, la Corte ha affermato che sono gli Stati e non il Governo Federale, ad essere i garanti finali della privacy individuale. Questo in virtù del principio per il quale i singoli Stati possono scegliere di accordare, tramite le proprie Costituzioni, maggiori diritti ai cittadini rispetto a quelli previsti dalla Costituzione Federale. Secondo un'immagine suggestiva ed efficace, *"in any given state, the federal Constitution represents the floor for basic freedoms; the state constitution, the ceiling*[54]*."*

[48] *Carey v. Population Servs. Int'l*, 431 U.S. 678 (1977)
[49] *Bowers v. Hardwick*, 478 U.S. 186 (1986)
[50] Kathleen Anne Ward, *Williams vs. Attorney General of Alabama: does a constitutional right to sexual privacy exist?,* Thomas Jefferson Law Review Fall2008, Vol. 31 Issue 1, p1-24, 24p
[51] *Lawrence vs. Texas* , 539 U.S. 558, 578 (2003)
[52] Whalen v. Roe, 429 U.S. 589 (1977)
[53] *Katz v. United States*, 389 U.S. 347 (1967)
[54] *Traylor v. State*, 596 So. 2d 957, 962 (Fla. 1992)

Per questi motivi, nel periodo tra il 1968 e il 1980, diversi stati quali la Florida[55], la California[56], l'Alaska[57] e il Montana[58] hanno provveduto ad aggiornare le rispettive Costituzioni statali inserendovi delle specifiche clausole relative alla tutela della privacy[59].

Se il concetto federale di privacy è rimasto dormiente, la relativa concezione statale si è resa invece più dinamica, in risposta alle mutevoli esigenze di una società in costante evoluzione. Sulla scorta di queste considerazioni non appare affatto sorprendente che alcuni stati si siano spinti sino a riconoscere la legittimità costituzionale dei matrimoni civili tra persone dello stesso sesso e che i cittadini, dal canto loro, abbiano preso a ricercare la tutela della loro privacy all'interno dei tribunali statali, divenuti maggiormente capaci di dare risposte alle loro esigenze di tutela.

In conclusione, dopo un periodo di iniziale attivismo la Corte Suprema americana si è dimostrata sempre più restia ad estendere i confini del diritto alla privacy, la cui esatta collocazione nell'ambito della Costituzione federale rimane ancora, per certi versi, poco chiara. Per questi motivi la tutela della privacy, che ha visto la luce nelle corti statali, è tornata ad essere una prerogativa costituzionale dei singoli Stati americani i quali, nella voluta inerzia della Corte Suprema, hanno adottato il relativo modello federale per poi rimodellarlo ed estenderlo ad ulteriori aree di applicazione[60].

4. Considerazioni generali sulla legislazione federale degli Stati Uniti d'America

Nei capitoli precedenti si è descritta l'evoluzione del dibattito giurisprudenziale in tema di tutela della privacy sviluppatosi a seguito della storica affermazione del "*right to be let alone*" con la *law review* di S. Warren e L. Brandeis. In questo capitolo verrà aperto, invece, uno

[55] Constitution of the State of Florida, Article I, Section 23 "*Every natural person has the right to be let alone and free from governmental intrusion into the person's private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by law*".

[56] Constitution of the State of California § 1. "*All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy*".

[57] The Constitution of the State of Alaska § 22. Right of Privacy *"The right of the people to privacy is recognized and shall not be infringed. The legislature shall implement this section. [Amended 1972]"*

[58] The Constitution of the State of Montana § 10. Right of privacy. "*The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest*".

[59] Kathleen Anne Ward , nota 50

[60] *Idem*

spaccato sulla legislazione federale americana. La premessa è, a mio avviso, indispensabile per comprendere appieno le divergenze con il sistema europeo.

Com'è noto gli Stati Uniti d'America sono uno Stato federale. Ciò comporta che, a rigore, coesistano in seno ad esso tanti sistemi giuridici quanti sono gli Stati federati, con l'aggiunta dell'ordinamento giuridico federale. Si può, dunque, affermare che negli USA vi siano attualmente ben 51 sistemi giuridici distinti[61].

La Costituzione federale, vera e propria chiave di volta del sistema giuridico americano, assegna alla competenza legislativa del Congresso un certo numero di materie indicate dalla sezione 8 dell'art. I. Tra queste materie, le più importanti sono quelle ricomprese nella cd. *commerce clause*, la materia delle insolvenze (*bankruptcy*), i diritti sulle opere dell'ingegno e, per altri versi, le materie che corrispondono al nostro diritto della navigazione e dei trasporti (*marittime and admiralty*).

Inoltre, il XIV emendamento ha introdotto un principio di federalizzazione dei diritti fondamentali contenuti nel Bill of Rights, in virtù del quale "*nessuno Stato emanerà o farà vigore ad alcuna legge che restringa i privilegi o le immunità dei cittadini degli Stati Uniti; così pure nessuno Stato priverà alcuna persona della vita, della libertà o della proprietà se non in seguito a regolare procedimento legale, né rifiuterà a chicchessia nei limiti della sua giurisdizione l'eguale protezione delle leggi*"[62].

Il sistema di ripartizione delle competenze legislative a livello costituzionale è, infine, completato dal X emendamento. Tale norma di chiusura prevede una clausola di riserva in virtù della quale tutti i poteri non delegati al sistema federale vengono mantenuti dai singoli Stati[63].

Storicamente il *trend* della produzione normativa da parte del Congresso federale non è mai stato uniforme. Si è passati, infatti, da un'attività legislativa molto tenue durante l'800 ad un notevole incremento della produzione normativa a partire dagli anni 30 del primo novecento[64]. Il Congresso è, poi, intervenuto massicciamente durante gli anni 80 nel campo della tutela dell'ambiente e dei consumatori, creando Agenzie federali con compiti specifici (basti pensare alla *Federal Aviation Administration* o alla *Transportation Security*

[61] Antonio Gambaro, Rodolfo Sacco in "*Sistemi Giuridici Comparati*", Torino 2002, pp. 201 e ss.

[62] U.S. Constitution, 14th Amendment *"All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws".*

[63] U.S. Constitution, 10th Amendment "*The powers not delegated to the United States by the Constitution, nor prohibited by it to the States, are reserved to the States respectively, or to the people*".

[64] in coincidenza con il New Deal dell'amministrazione Roosevelt

Administration di cui si è già detto) alle quali è stato delegato il potere di emanare *regulations* attuative degli scopi disegnati con legge[65]. Il tutto grazie anche all'interpretazione estensiva che la Corte Suprema ha dato alla "*commerce clause*", la quale viene intesa nel senso che è materia federale tutto quanto attiene alla produzione ed allo scambio di beni e di servizi a raggio potenzialmente interstatale[66].

In tutte le materie rientranti nel blocco di competenza federale trova applicazione la cd. *supremacy clause*, un principio che ricorda molto quello del primato del diritto comunitario, alla luce del quale i giudici statali applicano il diritto federale con precedenza su quello statale. In altre parole la norma federale prevale su quella statale eventualmente in contrasto[67]. Inoltre, nell'applicazione delle norme federali il giudice statale deve, altresì, attenersi ai precedenti giurisprudenziali federali. Pertanto, una pronuncia della Corte Suprema Federale sarà considerata come precedente vincolante per tutti i giudici federali o statali i quali debbano applicare la regola o il principio di diritto federale su cui la Corte Suprema si è pronunciata[68].

Tuttavia, nonostante la crescita torrenziale della legislazione congressuale dei tempi recenti, il diritto federale ha sempre mantenuto "natura interstiziale" [69] conservando, cioè, uno scopo ed una portata limitati. Esso si basa su rapporti giuridici fondati e regolamentati dal diritto statale che sovverte solamente quando la cosa sia resa necessaria per scopi particolari. In particolare gli Stati possono intervenire legislativamente anche nelle materie assegnate al potere federale nella misura in cui un qualche aspetto non sia compiutamente regolato dalla legislazione federale. Può, infatti, avvenire che una legge del Congresso stabilisca certi diritti ma taccia sui rimedi, residuando quindi un margine di intervento normativo da parte degli Stati.

Fatte queste premesse, si può agevolmente comprendere le ragioni per cui il quadro normativo americano sulla tutela della privacy risulti così frammentario e disomogeneo. Come affermato dalla Corte Suprema in *Katz vs. United States*, infatti i singoli stati sono liberi di attribuire ai cittadini maggiori diritti di quelli previsti dalla legislazione federale[70]. La conseguenza di tutto ciò é che la protezione della privacy risulta differenziata non soltanto da Federazione a Stato, ma anche da Stato a Stato.

[65] Antonio Gambaro, Rodolfo Sacco, nota 61
[66] Idem
[67] Ibidem
[68] Ugo Mattei, nota 5
[69] Idem
[70] *Katz v. United States*, nota 53

Nei capitoli precedenti si è anche accennato al fatto che la legislazione federale sulla privacy si caratterizza per il suo approccio "settoriale". In particolare, sebbene il problema della privacy sia particolarmente sentito negli USA e nonostante esista anche una copiosa letteratura giuridica sul tema manca una legge generale che, come nel caso della Direttiva Europea, disciplini integralmente il trattamento dei dati personali[71]. Ciò fa si che diversi settori dell'economia americana non siano coperti da una legislazione che tuteli la privacy dei cittadini.

A parere di chi scrive, si deve ritenere che questo diverso approccio legislativo, frutto di esperienze e di tradizioni giuridiche diverse, sia all'origine della controversia tra USA e UE in materia di PNR. Come evidenziato da più autori, tra le principali ragioni per cui il livello di tutela dei dati personali negli USA è stato ritenuto inadeguato da parte degli organi europei deve annoverarsi proprio la mancanza, nell'ordinamento giuridico di quel paese, di una *comprehensive legislation* a tutela della privacy, avente contenuti e *standards* di protezione equivalenti a quelli europei.

Scopo del capitolo che segue è quello di offrire una panoramica dei principali strumenti legislativi federali a tutela della privacy. Naturalmente, per esigenze di compatibilità con la presente opera, la trattazione dei singoli istituti sarà limitata agli aspetti essenziali e di maggiore interesse.

5. La tutela della privacy nella legislazione federale

Durante gli anni settanta la crescita in dimensioni della società americana unita ai progressi dell'informatica - che ha comportato la sostituzione dei registri e degli archivi cartacei con i più moderni ed efficienti sistemi automatizzati di raccolta - ha contribuito a rafforzare l'esigenza di una regolamentazione dell'attività di *record-keeping*.

Nel 1972 il *Department of Health, Education and Welfare* creava, quindi, un comitato consultivo per studiare i sistemi automatizzati di gestione dei dati utilizzati dalle agenzie governative. Il parere di quest'ultimo circa le buone pratiche di informazione da incorporarsi in tutti i sistemi di trattamento, venne codificato quasi alla lettera nel successivo intervento legislativo del Congresso americano sulla materia[72]: .

[71] Dorothee Heisenberg, nota 6

[72] avutosi con l'emanazione del Privacy Act del 31 dicembre 1974

Tra i principi enucleati dal comitato consultivo del *Department of Health, Education and Welfare* ricordiamo[73]:

1. Il principio di trasparenza: l'esistenza di sistemi di raccolta e di banche dati che contengano dati personali deve essere resa nota al pubblico, insieme con una descrizione degli scopi e delle finalità della raccolta.
2. Il principio della partecipazione individuale: gli individui devono avere diritto a prendere visione di tutti i dati che li riguardano. Devono, altresì, essere messi in condizione di rettificare o cancellare i dati che non sono aggiornati, accurati, rilevanti o completi.
3. Il principio di limitazione della raccolta: vi devono essere dei limiti alla raccolta dei dati personali. La raccolta deve avvenire con mezzi leali e legittimi e, ove possibile, con la conoscenza o il consenso del soggetto interessato.
4. Il principio della qualità dei dati: i dati personali devono essere rilevanti per gli scopi per i quali sono stati raccolti ed utilizzati. Devono essere accurati, completi ed aggiornati.
5. Il principio di finalità: I dati devono essere utilizzati solo per gli scopi specificati al tempo in cui furono collezionati. I dati non devono essere altrimenti pubblicati senza il consenso del soggetto interessato ovvero senza l'autorizzazione delle autorità legittime.
6. Il principio di sicurezza: i dati personali devono essere protetti da misure di sicurezza ragionevoli contro rischi di smarrimento, accesso non autorizzato, distruzione, alterazione o pubblicazione illegittimi ecc.
7. Il principio di responsabilità: i record-keepers devono essere responsabili dell'osservanza delle buone pratiche di informazione,

Come già accennato, nel 1974 il Congresso federale provvedeva ad emanare il Privacy Act, comportando una codificazione, quasi alla lettera, dei principi ora descritti.

L'intervento legislativo aveva come obiettivo proprio quello di tutelare i cittadini americani dal crescente numero di invasioni della privacy perpetrati dagli organi federali attraverso l'uso di sempre più sofisticati strumenti di raccolta informatica. Del resto, il *tort of invasion of privacy* elaborato dal *common law* delle corti statali sin dai primi del '900, offriva rimedi soltanto nei confronti delle invasioni della privacy da parte di altri soggetti privati ovvero delle autorità statali. Non offriva, invece, alcun rimedio qualora l'invasione della

[73] Hong Haeji, "*Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao*", in Akron Law Review, 2005, Vol. 38 Issue 1, p71-111, 41p

privacy provenisse da autorità federali[74]. Per questa ragione il Privacy Act ha visto la luce in un clima di deciso consenso politico in seno al Congresso americano, ed è stato caldeggiato anche dall'amministrazione Ford[75].

Tale strumento normativo, tutt'ora in vigore, trova applicazione nei confronti delle "*federal agencies*"[76] che detengono dati riferibili ad un individuo e che siano contenuti in un "*system of records*". In particolare, esso nasce dalla necessità di creare un equilibrio tra due opposte esigenze: quella di salvaguardare l'efficienza e il buon funzionamento del Governo federale e quella di garantire il diritto alla riservatezza dei cittadini.

A tal fine, il Privacy Act limita la facoltà degli organismi federali di raccogliere, gestire e pubblicare dati personali, sebbene con alcune eccezioni.

In sintesi il sistema di garanzie offerto dal Privacy Act è articolato sui seguenti principi:

1. diritto dell'individuo a controllare l'uso e la diffusione delle informazioni contenute nel suo "*record*"
2. diritto dell'individuo a visionare, correggere o aggiornare le informazioni che lo riguardano
3. disciplina e limitazione delle ipotesi di raccolta, conservazione, uso e diffusione dei dati personali
4. previsione di meccanismi di responsabilità civile per le violazioni delle disposizioni del Privacy Act.

La prima clausola di garanzia implica il divieto per la *federal agency* di pubblicare o diffondere i dati personali di un soggetto se non in forza di una sua richiesta scritta o dietro consenso di quest'ultimo. Questo generico divieto di diffusione dei dati senza consenso é, tuttavia, soggetto a numerose eccezioni tra cui, segnatamente, quelle previste dal *Freedom of Information Act*. Tra queste ricorderemo il trattamento o il trasferimento di dati per motivi statistici, per finalità di ordine pubblico, di pubblica emergenza o per l'esistenza di un mandato giudiziario. Un'ulteriore eccezione è data poi dal "*routine use*" dei dati da parte delle federal agencies.

La seconda clausola di garanzia comporta il diritto del singolo ad avere accesso ai propri dati al fine di consentirgli la correzione, la rettifica ovvero l'aggiornamento dei medesimi. E',

[74] Frederick Z. Lodge, "*Damages under the Privacy Act of 1974: Compensation and deterrence*", in Fordham Law Review, March 1984, Vol. 52, p611-636, 26p

[75] Todd Robert Coles, "*Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption*", in American University Law Review, Winter 1991, Vol. 40, p957-1002, 46p

[76] con ciò intendendosi, fra l'altro, *l'executive branch*, le forze armate e i *federal departments*.

altresì, prevista la possibilità di fare ricorso alle Corti federali qualora la Federal Agency non ottemperi alla richiesta di rettifica.

La terza clausola è volta a limitare le facoltà di raccolta, mantenimento, utilizzo e diffusione dei dati personali. Le federal agencies sono autorizzate a raccogliere soltanto quelle informazioni che sono necessarie alle finalità perseguite mediante la raccolta stessa. Ove possibile, dette informazioni devono essere raccolte direttamente dall'interessato e, in ogni caso, devono essere mantenute in forma accurata e completa. Le federal agencies devono, inoltre, pubblicare un'informativa nel Federal Register[77] indicando tutti i *system of records* custoditi presso di esse e devono, altresì, mantenere un prospetto accurato di tutte le operazioni di pubblicazione e/o diffusione dei dati con l'indicazione delle relative causali. Le federal agencies devono poi dotarsi di un codice di condotta per i propri funzionari incaricati della gestione dei system of records.

La quarta clausola prevede, infine, dei meccanismi di tutela risarcitoria civile. In particolare, ai sensi del Privacy Act, l'azione civile di danno è esperibile innanzitutto nel caso in cui la federal agency non ottemperi alla richiesta di rettifica o di aggiornamento dei dati presentata dall'interessato.

Allo stesso modo, l'azione civile è ammissibile anche qualora la federal agency non permetta all'interessato di accedere ai propri dati ovvero qualora dalla conservazione inaccurata o negligente dei medesimi derivi un pregiudizio per l'interessato.

Più in generale, il Privacy Act prevede, comunque, che l'azione civile possa essere esperita a fronte di qualsiasi violazione delle sue disposizioni da cui sia derivato, quale conseguenza diretta, un danno per il singolo.

Tuttavia, il livello di tutela della riservatezza offerta dal Privacy Act presenta anche delle vistose lacune.

La prima deriva, anzitutto, dal suo campo di applicazione. Infatti, il Privacy Act si applica soltanto all'attività delle federal agencies. Si tratta, cioè di una legge che tutela la privacy dei cittadini soltanto nei confronti dell'attività degli organi del governo federale. Sono esclusi dal suo campo di applicazione gli enti statali come anche i soggetti privati. E, come osservato in dottrina[78], non tutti gli Stati americani sono dotati di una legislazione su modello del Privacy Act che tuteli i propri cittadini da analoghe invasioni della privacy da parte degli organi statali.

[77] Il Federal Register è una gazzetta ufficiale del governo federale degli Stati Uniti che viene pubblicata con cadenza giornaliera, esclusi i giorni festivi. E' una fonte di cognizione pubblica dell'attività federale, accessibile a chiunque.
[78] Amy S. Scarborough , "*Nevada needs a Privacy Act: how nevadans are particularly at risk for identity theft*", in Nevada Law Journal, Spring 2007, Vol. 7 Issue 2, p640-663, 24p

Allo stesso modo, il Privacy Act riguarda solamente il trattamento dei dati appartenenti a cittadini statunitensi o a persone che abbiano la residenza negli Stati Uniti. E non interessa, poi, qualsiasi attività di raccolta o di trattamento di dati da parte di una federal agency ma soltanto l'attività di quelle federal agencies che custodiscono un system of records.

Infine, il regime di eccezioni al divieto di pubblicazione senza il consenso dell'interessato (previsto nel numero di dodici), costituisce un'ulteriore limitazione alla tutela offerta da questa legge[79]. Nel caso di diffusione indebita dei dati in violazione di tali disposizioni, i danneggiati sono confrontati a barriere procedurali considerevoli prima di poter azionare il rimedio innanzi alle corti federali. Infatti, su di essi grava l'onere della prova del danno, nonché un termine di decadenza di due anni dalla data dell'indebita pubblicazione per proporre l'azione. Inoltre, la diffusione pregiudizievole deve avere ad oggetto informazioni personali contenute in un *system of records* e tale diffusione deve essere avvenuta intenzionalmente.

[79] Julianne M. Sullivan, "*Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving*", in California Western Law Review 39 no2 395-412 Spr 2003

CAPITOLO II: LA TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA

1. Le origini del diritto alla privacy in Europa. La Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali.

La concezione europea di privacy quale diritto fondamentale della persona trae, con ogni probabilità, origine da ragioni di carattere storico.

Se si considera, infatti, che gli Stati Uniti d'America non hanno mai sperimentato la dittatura quale forma di governo, non pare si possano nutrire dubbi sul fatto che l'esperienza dei regimi nazi-fascisti del novecento abbia contribuito a rafforzare l'intensità con la quale, in Europa, viene avvertita l'esigenza di una forte tutela della sfera privata individuale.

D'altronde, la manipolazione dei dati personali "sensibili" a fini politici (si pensi alla razza, al credo religioso, all'affiliazione sindacale come pure all'orientamento sessuale) quale strumento per l'attuazione di una politica repressiva o razzista ha rappresentato una prassi generalizzata in seno a numerosi regimi autoritari europei. Basterà ricordare, nel caso dell'Italia, l'emanazione delle leggi razziali[80].

In Europa la prima forma di tutela specifica della privacy a livello regionale risale alla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (in prosieguo "CEDU"), firmata a Roma nel 1950, nel quadro della prima organizzazione regionale intergovernativa con vocazione universale sorta nel secondo dopoguerra: il Consiglio d'Europa.

Com'è noto la CEDU costituisce, al contempo, il primo dei grandi trattati di carattere generale in materia di tutela dei diritti della persona, nonché quello più avanzato sotto il profilo del sistema internazionale di controllo sul rispetto dei diritti tutelati, essendo l'unico a prevedere un meccanismo di garanzia che, allo stato attuale, é integralmente giurisdizionale[81].

L'art. 8 CEDU recita che

[80] vedi per tutte R.D.L. 15 novembre 1938, n. 1779 recante "*Integrazione e coordinamento in testo unico delle norme già emanate per la difesa della razza nella scuola italiana*"; R.D.L. 7 settembre 1938, n. 1381 recante "*Provvedimenti nei confronti degli ebrei stranieri*"; R.D.L. 29 Giugno 1939, n. 1054 recante "*Disciplina dell'esercizio delle professioni da parte dei cittadini di razza ebraica*".

[81] Marco Pedrazzi, "*La Convenzione Europea sui diritti umani e il suo sistema di controllo", in "La tutela dei diritti umani. Norme, garanzie e prassi*", a cura di Laura Pineschi, Milano 2006 p. 236.

"1. Ogni persona ha diritto al rispetto della sua vita private e familiare, del suo domicilio e della sua corrispondenza

2. Non può esservi ingerenza della pubblica autorità nell'esercizio di tale diritto se non in quanto tale ingerenza sia prevista dalla legge e in quanto costituisca una misura che , in una società democratica, é necessaria per la sicurezza nazionale, l'ordine pubblico, il benessere economico del paese, la prevenzione dei reati, la protezione della salute o della morale, o la protezione dei diritti e delle libertà altrui."

Come si noterà, questa disposizione è caratterizzata da un ambito di applicazione particolarmente vasto, tale da ricomprendere situazioni giuridiche e di fatto alquanto eterogenee. Esso include il diritto al nome, alla tutela della riservatezza ed all'autonomia personale, come pure la libertà di operare senza interferenze le scelte riguardanti la propria sfera privata quali l'orientamento e la vita sessuale.

Inoltre, l'art. 8 CEDU tutela, altresì, il diritto all'identità ed all'immagine, esistendo una zona di interazione della persona con i terzi, ancorché in contesto pubblico, che può ricadere nel campo di applicazione della nozione di "vita privata"[82]. Illuminante, in questo senso, é la pronuncia della Corte EDU sulla vicenda delle foto della principessa Von Hannover[83].

Da ultimo, nell'estensione dell'art. 8 CEDU, è compreso anche il diritto allo sviluppo delle relazioni sociali quale espressione della realizzazione della propria personalità[84], nonché la protezione dei dati personali.[85]

[82] Peck c. Regno Unito (*Ricorso n. 44647/98), sentenza del 28 gennaio 2003. Fattispecie relativa alla diffusione a mezzo stampa e televisiva di una sequenza tratta da telecamere a circuito chiuso che avevano ripreso un uomo mentre si aggirava per una strada di notte impugnando un grosso coltello (con l'intenzione, in realtà, di usarlo per tagliarsi le vene). La Corte stimava che, sebbene l'uomo si trovasse in un luogo aperto al pubblico, sussistevano comunque profili concernenti la protezione della vita privata dal momento in cui vi era stata una registrazione sistematica e permanente di detto materiale finalizzata alla successiva riproduzione.*

[83]Von Hannover c. Germania, (*Ricorso n. 59320/00), sentenza del 24 giugno 2004. Fattispecie relativa alla pubblicazione di alcune foto private della principessa Carolina di Monaco su varie riviste tedesche ritenuta legittima da parte della Corte Suprema Federale di Germania in quanto personaggio di rilevante interesse pubblico. La Corte EDU ha affermato, invece, la violazione dell'art. 8 CEDU osservando come la principessa, che non é titolare di alcuna funzione ufficiale in seno allo stato monegasco, fosse stata fotografata esclusivamente in momenti riguardanti la sua vita privata. Di conseguenza, anche la principessa doveva ritenersi titolare, in tale riservato contesto, di una ragionevole aspettativa al rispetto della propria privacy non sussistendo, nella specie, alcun apprezzabile interesse pubblico alla pubblicazione delle fotografie*.

[84] Corte EDU, caso Niemietz c. Germania *(Ricorso n. 13710/88), sentenza del 16 dicembre 1992, par. 29*

[85] Corte EDU, caso Z. c. Finlandia *(Ricorso n. 22009/93) sentenza del 25 febbraio 1997, par. 5.*

L'art 8 CEDU si pone in stretta relazione anche con altre disposizioni della medesima Convenzione, in particolare quelle che disciplinano il diritto a contrarre matrimonio (art. 12 CEDU) e l'eguaglianza dei coniugi (art. 5 Protocollo n. 7). Sotto questo profilo, come si vedrà in prosieguo, il riferimento al diritto "*al rispetto della vita privata e familiare*" piuttosto che "*al diritto alla vita privata e familiare*" rafforza l'idea che dall'art. 8 derivino, oltre a obblighi "negativi" per gli Stati di astenersi da qualsivoglia ingerenza ingiustificata nel godimento dei diritti ivi riconosciuti, anche obblighi "positivi" volti ad assicurarne l'effettivo rispetto, nonché a prevenire e contrastare eventuali interferenze da parte di terzi[86].

Nei paragrafi che seguono verrà illustrata, anzitutto, l'evoluzione della giurisprudenza della Corte Europea dei Diritti dell'Uomo sulla disposizione in esame. Iniziare con tale premessa non è affatto una scelta casuale, almeno per due validi motivi.

In primo luogo perché tale giurisprudenza riveste un'indubbia importanza ai fini della comprensione della portata effettiva della disposizione in commento, nonché delle problematiche giuridiche sottese alla sua applicazione pratica.

In secondo luogo perché, considerato che anche l'Unione Europea riconosce e garantisce i diritti inviolabili dell'Uomo quale riconosciuti dalla CEDU[87], non si può certo prescindere dall'interpretazione che di tali diritti viene fatta proprio dalla Corte Europea di Strasburgo. Infine, si deve, altresì, tenere in considerazione il fatto che la relativa giurisprudenza riveste un rinnovato interesse anche alla luce dell'eventuale adesione dell'Unione Europea in quanto tale alla CEDU, quale sancita dal Trattato di Lisbona.

2. La giurisprudenza della Corte Europea dei Diritti dell'Uomo. La nozione di "dati personali" e di "dossier".

Come si accennava poc'anzi, la giurisprudenza della Corte Europea dei Diritti dell'Uomo (in prosieguo "Corte EDU") ha contribuito ad approfondire ulteriormente la nozione di vita privata di cui all'art. 8 CEDU.

[86] Cesare Pitea, "*L'interpretazione evolutiva del diritto al rispetto della vita privata e familiare in materia di libertà sessuale e di tutela dell'ambiente*", in "*La tutela dei diritti umani. Norme, garanzie e prassi*", a cura di Laura Pineschi, Milano 2006 p. 428

[87] A partire dal Trattato di Maastricht del 1992. Dato che la Comunità Economica Europea vede la propria nascita senza una reale competenza in materia di diritti fondamentali, per molto tempo l'unica voce in capitolo sarà proprio quella della Corte Europea dei Diritti dell'Uomo.

Sulla disposizione in esame, infatti, esiste un numero elevatissimo di pronunce della Corte di Strasburgo, a riprova della particolare vastità del suo campo di applicazione.

Per quanto di interesse ai fini della presente ricerca, si cercherà necessariamente di circoscrivere l'analisi alle pronunce maggiormente rilevanti in tema di protezione dei dati personali.

I casi sottoposti all'attenzione della Corte in tale materia sono stati numerosissimi, ed hanno interessato, durante il corso degli anni, situazioni e problematiche assai eterogenee. A ben vedere infatti, queste ultime spaziano dalle intercettazioni telefoniche e di corrispondenza nell'ambito delle indagini di polizia, sino alle domande tese ad ottenere l'accesso e la rettifica dei dati contenuti in un dossier.

Ciò premesso, occorre sin d'ora evidenziare come, secondo l'insegnamento della Corte, nel concetto di "dati personali" rientrino, accanto ai semplici dati anagrafici, anche le impronte digitali e i dati genetici. Invero, anche la conservazione a tempo indeterminato del DNA di una persona costituisce interferenza nella vita privata e familiare di quest'ultima, dal momento in cui i campioni di DNA contengono numerose informazioni di carattere sensibile, segnatamente quelle relative alla salute. Tali campioni racchiudono, altresì, un codice genetico unico che riveste una grande importanza per l'interessato e che permette, tra le altre cose, di risalire anche all'origine etnica del medesimo[88].

Inoltre, sempre secondo la giurisprudenza della Corte EDU, la semplice memorizzazione, da parte di un'autorità pubblica, dei dati relativi ad un individuo costituisce di per sé un'ingerenza ai sensi dell'art. 8 CEDU, non avendo rilevanza alcuna l'effettiva od ulteriore utilizzazione di questi ultimi. Tale principio, originariamente affermato nel caso *Leander c. Svezia* del 1987[89] é, successivamente, entrato a far parte integrante dell'orientamento consolidato della Corte[90].

Il caso Leander aveva, infatti, ad oggetto la vicenda di un cittadino svedese iscritto nel registro delle persone pericolose per la sicurezza nazionale in ragione della sua previa militanza politica in un partito estremista. Al ricorrente era stata, conseguentemente, negata la possibilità di accedere ad un impiego pubblico.

Il caso Leander merita particolare attenzione in quanto in esso la Corte ha, per la prima volta, precisato la nozione di "*dossier personale*" affermando, appunto, come la mera creazione e conservazione, da parte di un'autorità pubblica, di un registro contenente i dati

[88] S. e Marper c. Regno Unito (*Ricorsi nn. 30562/04 e 30566/04), sentenza del 4 dicembre 2008*

[89] Leander c. Svezia (*Ricorso n. 9248/81), sentenza del 26 marzo 1987*

[90] Cfr. *ex plurimis* Amann c. Svizzera, (*Ricorso n. 27798/95), sentenza del 16 febbraio 2000*; Kopp c. Svizzera (13/1997/797/1000), *sentenza del 25 marzo 1998*; Segerstedt-Wiberg e altri c. Svezia, *sentenza del 6 giugno 2006.*

personali di una persona costituisca un'ingerenza nel diritto alla vita privata di quest'ultima e ciò a prescindere dalla concreta utilizzazione di tali informazioni[91].

In ogni caso, la giurisprudenza della Corte si è concentrata sopratutto sul meccanismo che legittima le ingerenze statali nella vita privata. L'art. 8 CEDU, infatti, é strutturato in due paragrafi, il primo contenente l'esplicitazione dei diritti dell'individuo, mentre il secondo elenca le condizioni necessarie perché lo stesso possa essere limitato in presenza di un interesse della collettività.

A tal fine, come si ricorderà, occorre che l'interferenza sia prevista con legge, sia necessaria in una società democratica e persegua uno degli scopi legittimi individuati dalla norma. Questi sono, pertanto, i necessari passaggi logici che la Corte EDU compie ogniqualvolta le venga sottoposta un questione sotto il profilo dell'art. 8 CEDU.

3. Sulla necessità della previsione con legge. Il principio della "qualità" della legge.

Come si accennava poc'anzi, l'interferenza statale nel diritto di cui all'art. 8 CEDU è ammessa, anzitutto, soltanto se prevista con legge.

Il concetto di "legge" ai sensi della disposizione testé citata è stato chiarito dalla Corte EDU nel caso *Malone c. Regno Unito* del 1984[92], avente ad oggetto la vicenda di un mercante d'arte irlandese accusato di ricettazione e, conseguentemente, sottoposto ad intercettazioni telefoniche e della corrispondenza da parte della polizia inglese. La Corte, richiamando la propria giurisprudenza sul punto[93], ha innanzitutto affermato che per "legge" deve intendersi "*sia il diritto scritto che il diritto non scritto*", ivi compresa la prassi amministrativa[94].

Tuttavia, la Corte ha affermato che, nonostante sia pacifico che l'ingerenza statale nel diritto alla vita privata debba trovare "*fondamento nel diritto interno*", ciò non significa che la legge in questione possa limitarsi ad essere "meramente conforme" al diritto nazionale. Al contrario, la Corte ha teorizzato il principio della "qualità" della legge, che postula l'esigenza che la stessa sia sufficientemente accessibile da parte dei cittadini.

[91] Tuttavia in quel caso la Corte affermava la non violazione dell'art. 8, rilevando come le autorità nazionali godano di un margine di discrezionalità che dipende, oltre che dalla finalità legittima perseguita, anche dal carattere proprio dell'ingerenza praticata, atteso che la Convenzione non garantisce in quanto tale l'accesso al pubblico impiego.
[92] Malone c. Regno Unito (*Ricorso n. 8691/79), sentenza del 2 agosto 1984*
[93] Silver ed altri c. Regno Unito del 25 marzo 1983 (serie A n° 61, pp. 32-33, par. 85) ; Sunday Times c. Regno Unito, sentenza del 26 aprile 1979
[94] Cfr. Leander c. Svezia par. 51

A detta della Corte "*il cittadino deve cioé poter disporre di informazioni sufficienti nelle circostanze di causa, sulle norme giuridiche applicabili a una fattispecie specifica. In secondo luogo, si può considerare legge soltanto una norma enunciata con sufficiente precisione e tale da permettere al cittadino di regolare la propria condotta e metterlo in condizione di poter prevedere con ragionevolezza le conseguenze che possono derivare da una specifica azione*[95]*"*. In altre parole, la Corte Edu, afferma che l'art. 8 par. 2 non attiene tanto al concetto di qualità "legge" in senso formale, quanto al concetto di qualità della legge in senso sostanziale.

La Corte enuclea, perciò, due distinti criteri che debbono essere rispettati affinché la legge soddisfi i parametri qualitativi ora descritti: da un lato il criterio di accessibilità (nel senso di concreta conoscibilità della legge da parte dei cittadini), dall'altro il criterio di prevedibilità (nel senso che la legge deve permettere al cittadino di poter ragionevolmente prevedere le conseguenze che possono derivare da una specifica azione). Si comprende come, in quest'ottica, un'intercettazione telefonica adottata in maniera conforme al diritto interno possa benissimo risultare illegittima alla luce della Convenzione qualora la norma nazionale posta a fondamento della sua applicazione non sia sufficientemente accessibile da parte dei potenziali destinatari[96].

Nel caso Malone la Corte supera, dunque, le obiezioni avanzate del Governo britannico, secondo cui gli imperativi della Convenzione, quanto alla nozione di prevedibilità della legge, non possono essere gli stessi nel caso specifico delle intercettazioni telefoniche, posto che le indagini di polizia devono poter contare su un margine ragionevole di segretezza e di sorpresa. Sulla questione la Corte osserva, invece, che la nozione di prevedibilità non comporta affatto l'obbligo di consentire ai cittadini di prevedere in ogni momento se le proprie comunicazioni vengono intercettate. Al contrario, essa implica soltanto che la legge debba indicare, in termini sufficientemente chiari, sotto quali circostanze e in virtù di quali condizioni i pubblici poteri sono autorizzati ad operare detta ingerenza nella vita privata e nella corrispondenza.

In altre parole la legge deve limitarsi a definire l'estensione e le modalità di esercizio di tale potere con precisione sufficiente, tenuto conto dello scopo legittimo perseguito, al fine di fornire all'individuo una protezione adeguata contro l'arbitrio[97]. Tale principio viene

[95] Malone c. Regno Unito, par. 66

[96] Khan c. Regno Unito, (*Ricorso n. 35394/97), sentenza del 12 maggio 2000*

[97] Cfr. ex plurimis Malone c. Regno Unito, par. 68; Wisse c. Francia, sentenza del 20 dicembre 2005; A. c. Francia, sentenza del 23 novembre 1993; P.G. e J.H. c. Regno Unito, sentenza del 25 settembre 2001; Van Vondel c. Paesi Bassi, sentenza del 25 ottobre 2007; Vetter c. Francia, sentenza del 31 maggio 2005; Taylor-Sabori c. Regno Unito, sentenza del 22 ottobre 2002. In tutti questi casi la Corte valuta con molto rigore l'esistenza di una legge chiara che

successivamente affermato anche dalla successiva giurisprudenza della Corte[98], la quale estende la tutela prevista dall'art. 8 CEDU anche alle conversazioni telefoniche professionali[99].

La sentenza in esame merita, inoltre, di essere segnalata in quanto prende posizione sulla questione del cd. "c*omptage*"[100]. Il governo inglese osservava come il comptage, in quanto non comportante l'ascolto del contenuto della conversazione, non avrebbe dato luogo ad alcuna ingerenza nel diritto di cui all'art. 8 CEDU. La Corte rilevava, al contrario, che nelle informazioni così raccolte figuravano dati, quali i numeri di telefono dei destinatari che formavano, invece, parte integrante delle conversazioni telefoniche private. Rivelare tali informazioni alla polizia senza il consenso dell'interessato avrebbe costituito violazione di un diritto consacrato dalla CEDU[101].

Particolare attenzione merita, sul punto, anche l'opinione concordante del giudice Pettiti[102], secondo il quale la Corte, nel caso Malone, avrebbe potuto cogliere l'occasione per pronunciarsi con maggiore precisione circa la compatibilità del modello inglese con l'art. 8 CEDU. Tradizionalmente, infatti, il diritto inglese prevedeva che ogni decisione riguardante la disposizione e l'utilizzo delle intercettazioni telefoniche fosse rimessa al potere esecutivo, senza che fosse previsto alcun controllo da parte dell'autorità giudiziaria.

Nel merito il giudice Pettiti osservava come la pratica degli ascolti polizieschi conduceva a costituire dei dossier a carico che rischiavano poi di privare di efficacia i meccanismi di protezione dell'equo processo sanciti dall'art. 6 CEDU, fortificando delle presunzioni di colpevolezza. Invero, l'ascolto e l'intercettazione esigono delle contromisure: diritto all'accesso da parte della persona posta sotto ascolto allorché la fase giudiziaria termini con un non luogo a procedere o un proscioglimento, nonché diritto alla cancellazione o alla restituzione dei nastri.

---

disciplini puntualmente le modalità dell'utilizzo, da parte delle autorità pubbliche, di strumenti di intercettazione telefonica o ambientale, ravvisando la violazione dell'art. 8 CEDU ogniqualvolta detta legge sia inesistente o poco chiara.

[98] Kruslin c. *Francia (Ricorso n°11801/85), sentenza del 24 aprile 1990*

[99] Kopp c. *Svizzera (13/1997/797/1000), sentenza del 25 marzo 1998*, in tema di intercettazioni telefoniche presso uno studio legale; Copland c. Regno Unito, *sentenza del 3 aprile 2007.*

[100] Misura oggi rimpiazzata dall'acquisizione dei tabulati telefonici, un tempo prevedeva l'installazione di un meccanismo (un contatore combinato con una stampante) che registrava i numeri di telefono composti e la durata delle chiamate ma non il contenuto delle conversazioni.

[101] Malone c. Regno Unito, par. 84

[102] Cfr. Malone c. Regno Unito, opinione concordante del giudice Pettiti

4. Sulla necessità in una società democratica. La proporzionalità dell'ingerenza allo scopo legittimo perseguito.

Come è già stato detto, oltre ad essere prevista con legge, l'interferenza statale deve soddisfare un ulteriore requisito: la necessità in una società democratica. Tale requisito, come si vedrà, comporta un giudizio di bilanciamento tra il diritto del singolo e la finalità legittima perseguito dai pubblici poteri. Inoltre, detto bilanciamento di valori implica, altresì, un vaglio circa la proporzionalità della misura rispetto alla finalità legittima perseguita.

Nel caso *Klass c. Germania*[103] del 1976, avente ad oggetto una legge della Repubblica Federale di Germania che, ai tempi di Guerra Fredda, imponeva limitazioni alla segretezza della corrispondenza e delle telecomunicazione quale misura di contrasto al terrorismo e allo spionaggio, la Corte ha affermato il principio della stretta interpretazione del regime delle eccezioni al divieto di ingerenza previsto dalla disposizione in esame.

Secondo quanto affermato dalla Corte, gli Stati contraenti non dispongono di un margine illimitato di discrezionalità al fine di assoggettare a misure di sorveglianza segreta le persone sottoposte alla loro giurisdizione, potendo simili interventi legislativi minare o addirittura distruggere proprio quel regime di democrazia che intendono difendere[104] . Infatti, "*il potere di sorvegliare i propri cittadini, caratteristico dello Stato di polizia, non è tollerabile ai sensi della Convenzione se non nei limiti di quanto strettamente necessario alla salvaguardia delle istituzioni democratiche*" [105].

L'esigenza di un esame rigoroso del sistema della proporzionalità dell'ingerenza allo scopo legittimo perseguito viene affrontato, invece, dalla Corte con riferimento ai dati personali riguardanti lo stato di salute delle persone nel caso *Z. c. Finlandia*[106] . Detto caso ha riguardato il ricorso della moglie di un uomo malato di AIDS, accusato di essere l'autore di diversi stupri. Durante il processo per violenza sessuale svoltosi in patria a carico di quest'ultimo, infatti, non appena è emersa la sua condizione di malato di AIDS, veniva disposta l'acquisizione della relativa cartella clinica che conteneva, però, informazioni suscettibili di rivelare il fatto che della medesima patologia era affetta anche la di lui moglie,

[103] Klass v. Repubblica Federale di Germania, *sentenza del 6 settembre 1978*

[104] Klass v. Repubblica Federale di Germania, par 49 «(…) *les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction. Consciente du danger, inhérent à pareille loi, de saper, voire de détruire, la démocratie au motif de la défendre, elle affirme qu'ils ne sauraient prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure jugée par eux appropriée (…) » .*

[105] Klass v. Repubblica Federale di Germania par 42. In ogni caso, nel caso Klass la Corte Edu ha concluso per la non violazione dell'art. 8 CEDU in quanto la legge tedesca è stata ritenuta come necessaria in una società democratica per sicurezza nazionale, la difesa dell'ordine e la prevenzione dei crimini.

[106] Z. c. Finlandia (ricorso n. 22009/93) sentenza del 25 febbraio 1997

persona non coinvolta a nessun titolo nel giudizio penale in quanto rifiutatasi di deporre come testimone in dibattimento.

Nel caso *Z. c. Finlandia* la Corte ha osservato come il rispetto del carattere confidenziale delle informazioni riguardanti la salute costituisca un principio essenziale comune a tutti i Paesi che hanno ratificato la Convenzione. Esso è fondamentale non soltanto per proteggere la privacy dei malati, ma altresì per preservare la loro fiducia nei confronti del personale medico e dei servizi sanitari in generale.[107] Senza una tale protezione le persone bisognose di cure mediche potrebbero essere dissuase dal fornire le informazioni di carattere personale ed intimo necessarie alla prescrizione del trattamento appropriato e persino di consultare un medico, il che potrebbe mettere in pericolo la loro salute ovvero, nel caso di malattie contagiose, quelle della collettività[108].

Pertanto, l'esigenza di proteggere la confidenzialità di tali informazioni pesa gravemente sulla bilancia allorquando si tratta di determinare se l'ingerenza é proporzionata allo scopo legittimo perseguito[109]. Alla luce di queste considerazioni la Corte ha ravvisato la violazione dell'art. 8 CEDU da parte della Finlandia nella pubblicazione, da parte della stampa, delle motivazioni della sentenza di condanna nella misura in cui ciò ha comportato la rivelazione dell'identità nonché della condizione di sieropositività della moglie del condannato. Agli occhi della Corte, infatti, tale ingerenza, seppur prevista con legge e perseguente uno scopo legittimo, non poteva dirsi necessaria in una società democratica .

5. Le obbligazioni "positive" derivanti dall'art. 8 CEDU. L'accesso ai dossier contenenti dati personali.

Come accennato in precedenza l'art. 8 CEDU si caratterizza per il fatto che, nonostante sia formulato "al negativo", dallo stesso possono derivare anche obblighi "positivi" a carico degli Stati volti ad assicurare l'effettivo rispetto dei diritti ivi previsti, nonché a prevenire e a contrastare interferenze illegittime da parte di terzi.

[107] Z. c. Finlandia, par. 95
[108] Cfr. Consideranda n. 165 della Raccomandazione n. R (89) 14, adottata dal Consiglio dei Ministri del Consiglio d'Europa il 24 ottobre 1989 recante "*Les incidences éthiques de l'infection VIH dans le cadre sanitaire et social*"
[109] Z. c. Finlandia, par. 96

Particolarmente emblematico, sotto questo profilo, è il caso *Gaskin vs Regno Unito*[110] del 1989. Si tratta della toccante vicenda di un minore britannico, orfano di madre, che era stato affidato alla tutela dei servizi sociali della città di Liverpool a seguito di una condanna per furto e rapina. Infatti, dato che il padre si era sempre rifiutato di occuparsi del piccolo, fin dalla più tenera età il sig. Gaskin aveva vissuto presso diverse famiglie affidatarie, conformemente alla legislazione inglese in materia di protezione dei minori.

Una volta divenuto maggiorenne il sig. Gaskin lamentava di essere stato, durante gli anni del suo affidamento, oggetto di ripetuti abusi e violenze che gli avevano comportato dei problemi a livello psicologico tali da ripercuotersi anche sulla sua vita adulta.

Il sig. Gaskin richiedeva, pertanto, ai servizi sociali della città di Liverpool (che conservavano un dossier strettamente confidenziale concernente la sua posizione), di permettergli l'accesso a tali informazioni al fine di scoprire dove, presso chi, ed in quali condizioni aveva vissuto, nella speranza di poter superare così i suoi problemi e conoscere la verità sul suo passato. L'accesso al dossier veniva autorizzato soltanto parzialmente, in quanto i Servizi Sociali ritenevano di dover osservare un dovere di confidenzialità nei confronti degli informatori anonimi[111].

Il sig. Gaskin faceva ricorso alla Corte d'Appello avverso tale decisione. La corte territoriale, tuttavia, confermava il provvedimento di parziale rigetto, ritenendo come consentire al Gaskin di accedere al relativo dossier non corrispondesse al pubblico interesse. Infatti, secondo la Corte d'Appello, tale accesso avrebbe comportato la necessità di rivelare l'identità di alcuni informatori e, pertanto, avrebbe scosso le basi del sistema britannico dei servizi sociali che si fonda largamente sulle informazioni confidenziali liberamente fornite alle autorità dai cittadini.

Nella vicenda Gaskin la Corte ha affermato l'esistenza di uno speculare obbligo "positivo" a carico degli Stati di consentire l'accesso degli interessati alle informazioni personali riguardanti la propria vita privata. Infatti, nel caso in esame la questione era tutt'altro che pacifica, dal momento in cui il Gaskin non lamentava che delle informazioni che lo riguardavano fossero state raccolte o utilizzate a suo detrimento. Al contrario egli ricorreva contro il rifiuto delle autorità pubbliche di consentirgli l'accesso alle informazioni che lo riguardavano.

[110] Gaskin c. Regno Unito (*Ricorso n. 10454/83), sentenza del 7 luglio 1989*

[111] Ai sensi della legislazione inglese tali informatori possono essere insegnanti, medici, agenti di polizia, genitori affidatari, assistenti sociali, ma anche soltanto amici o vicini di casa.

Il governo inglese affermava che i dossier riguardanti l'infanzia del sig. Gaskin non facevano parte in quanto tali della sua vita privata e familiare, poiché contenevano soltanto informazioni raccolte dalle autorità locali e, pertanto, né la loro costituzione né l'accesso alle relative informazioni ricadevano sotto l'ambito di applicazione dell'art. 8 CEDU. Inoltre, il Governo britannico eccepiva che la disposizione in esame, stante, la sua formulazione letterale, non ammetteva l'esistenza di presunte "obbligazioni positive".

La Corte, dal canto suo, esprimeva la propria contrarietà a tale tesi.

Di conseguenza, pur omettendo di prendere esplicitamente posizione sulla questione dell'esistenza di un diritto all'accesso ai dati personali, affermava che vi era stata violazione dell'art. 8 CEDU in quanto la decisione finale circa il diniego di autorizzazione ai dati del dossier non era stato adottata da parte di un organismo indipendente[112].

Sempre in tema di obbligazioni "positive" va ricordato anche il caso Rees c. Regno Unito[113] del 1986.

Alla sua nascita nel 1942, in Inghilterra, il sig. Rees presentava tutti i caratteri primari e biologici del sesso femminile e, come tale, figurava nell'atto di nascita col nome di Brenda Margaret Rees. Tuttavia, a partire dalla più tenera infanzia, lo stesso assumeva un comportamento prettamente maschile ed aveva un aspetto ambiguo. Dopo essersi sottoposto a diversi trattamenti medico-chirurgici volti alla modificazione del suo sesso, il sig. Rees cambiava il suo nome in Mark Nicholas Alban Rees ed otteneva anche il rilascio di un nuovo passaporto. Le autorità inglesi tuttavia, che pure si erano accollate i costi dell'operazione chirurgica, rifiutavano di modificare la menzione del sesso femminile che compariva ancora sul certificato di nascita.

Il sig. Rees ricorreva, pertanto, alla Commissione Europea dei Diritti dell'Uomo lamentando, tra l'altro, la violazione dell'art. 8 CEDU in ragione dell'imbarazzo e dell'umiliazione sofferta ogniqualvolta si vedeva costretto a esibire il certificato di nascita che, contenendo l'indicazione del suo sesso ufficiale, svelava la discordanza tra il suo aspetto e il suo sesso biologico. La questione non era oziosa in quanto, secondo il diritto allora vigente in Gran Bretagna il sig. Rees era comunque considerato come donna ai fini del matrimonio, dei diritti previdenziali, e anche in funzione di determinati lavori. L'esistenza di un atto di nascita non modificato poteva, inoltre, impedirgli di concludere certi contratti in qualità di uomo.

[112] Gaskin c. Regno Unito, par. 49

[113] Rees c. Regno Unito, (*Ricorso n. 9532/81), sentenza del 10 ottobre 1986*

Il sig. Rees chiedeva, pertanto, la modifica del certificato di nascita nonché la riservatezza di tale modifica, nel senso che la stessa non avrebbe dovuto essere comunicata a terzi.

La Corte Edu, sulla scorta della sua precedente giurisprudenza[114], afferma anche qui che nonostante l'art. 8 CEDU tenda a proteggere l'individuo contro le ingerenze dei poteri pubblici, esso può generare anche degli obblighi positivi in funzione di un rispetto efficace della vita privata e familiare ancorché soggetti ad un margine di apprezzamento da parte degli Stati contraenti. Tuttavia, trattandosi di una materia, quella del transessualismo, in cui il diritto è in una fase di transizione e dove non regna comunanza di vedute da parte degli Stati contraenti, la Corte ritiene che questi ultimi godano di un ampio margine di discrezionalità.

Di conseguenza, la Corte ritiene che nel Caso Rees non vi sia stata violazione dell'art. 8 CEDU nella misura in cui tale disposizione non può essere interpretata nel senso di imporre al Regno Unito né la modifica del sesso risultante dall'atto di nascita del ricorrente né, tantomeno, un'annotazione circa l'avvenuto cambio di sesso[115].

Un altro caso in cui sono venute in rilievo le obbligazioni positive dello Stato aveva come oggetto la pubblicazione, da parte di uno sconosciuto, di un annuncio su di un sito erotico di incontri per adulti a nome di un ragazzino di 12 anni[116].

A seguito della denuncia presentata dal padre del minore, la polizia chiedeva che l'Internet service provider fornisse l'identità della persona che aveva messo l'annuncio. Il Provider, tuttavia, rifiutava di fornire tali dati secondo quanto previsto dalla normativa finlandese. Tale decisione veniva, peraltro, confermata anche dal Tribunale Distrettuale di Helsinki che rigettava il ricorso della polizia, osservando come tra i reati per i quali la legge finlandese consentiva la divulgazione dell'identità nel campo delle telecomunicazioni non era ricompreso quello di sostituzione di persona. Conseguentemente, l'identità del soggetto che aveva messo l'annuncio esponendo il minore ad approcci da parte di pedofili non poté mai essere conosciuta.

La Corte in questo caso osservava come gli Stati debbano criminalizzare e perseguire i reati, specialmente quelli che vedono come vittima i minori e gli altri soggetti maggiormente bisognosi della protezione dello Stato. Nel caso di specie la Corte riteneva che la protezione

[114] Cfr. Abdulaziz, Cabales et Balkandali c. Francia del 28 maggio 1985, série A n° 94, pp. 33-34, par. 67

[115] Interessante è cmq l'opinione contraria dei giudici Bindschedler-Robert, Russo e Gersing, secondo cui il Regno Unito avrebbe potuto quantomeno inserire un'annotazione nel certificato di nascita del sig. Rees. In questo modo si sarebbe potuto salvaguardare sia la legittima aspettativa del sig. Rees in quanto rifletterebbe la sua situazione reale, che l'interesse pubblico soggiacente alla verità obiettiva di un fatto storico.

[116] K.U. c. Finlandia *(Ricorso n. 2872/02), sentenza del 2 marzo 2008*

concreta ed efficace del ricorrente richiedeva passi significativi volti ad identificare e perseguire l'autore dell'annuncio. Anche se la libertà di espressione e la confidenzialità delle comunicazioni sono questioni di primaria importanza e gli utenti di telecomunicazioni e servizi internet devono avere garanzia che la loro stessa privacy venga rispettata, tali garanzie non possono essere assolute e devono piegarsi all'occasione ad altri imperativi legittimi quali la prevenzione del crimine o la protezione dei diritti e delle libertà altrui. Conseguentemente la Finlandia aveva violato l'art. 8 CEDU sotto il profilo delle obbligazioni positive.

6. La Convenzione 108 del Consiglio d'Europa sul trattamento automatizzato dei dati a carattere personale.

Nell'ambito del Consiglio d'Europa è stata, altresì, stipulata la Convenzione n. 108 in materia di "protezione delle persone dal trattamento automatizzato dei dati a carattere personale"[117] (in prosieguo anche "*Convenzione 108*").

La finalità della Convenzione 108, quale enunciata nel relativo preambolo e nell'art. 1, é quella di conciliare l'esigenza della libera circolazione delle informazioni provenienti dall'elaborazione dei dati personali con il diritto fondamentale al rispetto della vita privata spettante ad ogni individuo, a prescindere dalla nazionalità e dalla residenza. La Convenzione ha, poi, come ulteriore obiettivo anche quello di stimolare gli Stati parte ad emanare delle norme interne di recepimento[118].

L'ambito di applicazione della Convenzione 108 è disciplinato dall'art. 3 par. 1 nella parte in cui precisa che la stessa si applica "*aux fichiers et aux traitements automatisés des données à caractère personnel dans le secteur public et privé"*. Come si può notare, l'applicabilità della Convenzione anche al settore privato, così come prevista dalla norma testé richiamata, scongiura l'eventualità che anche in relazione alla stessa sorgano i

[117] Convenzione del Consiglio d'Europa n. 108 recante "Protezione degli Individui in Relazione all'Elaborazione Automatica di Dati Personali", firmata a Strasburgo il 28 gennaio 1981.

[118] Chiara Bellini, "*Privacy Informatica. Una Ricostruzione di ampio respiro*", in "*Diritto della Famiglia e delle Persone*", anno 1999, fascicolo, 1 p. 459.

medesimi dubbi già emersi in passato circa l'estensibilità dell'art. 8 CEDU ai rapporti tra privati[119].

La Convenzione 108 indica, successivamente, i principi base a cui deve essere ispirata la gestione dei dati a carattere personale. Detti principi sono rivolti a garantire la proporzione tra contenuto dell'informazione e le finalità della stessa (art. 5), l'utilizzazione di informazioni sensibili (art. 6) e l'adozione di precauzioni tecniche (art. 7). Gli Stati parte si impegnano, poi, ad attuarli con la ratifica della Convenzione (art. 4 par. 2).

L'art. 8 prevede delle garanzie a favore della "*personne concernée*" affinché quest'ultima, una volta venuta a conoscenza di eventuali raccolte di dati personali che la interessano, possa richiedere la correzione delle notizie non veritiere, nonché disporre degli opportuni rimedi.

In particolare, lo spirito della Convenzione comporta l'adozione, da part degli Stati, di ogni misura affinché ciascun individuo possa venire a conoscenza del trattamento di dati personali che lo riguardano. Infatti, ciò costituisce presupposto indefettibile per l'esercizio delle garanzie previste dalla Convenzione.

Occorre, poi, ricordare che gli articoli 5 e 6 possono subire delle restrizioni soltanto nelle ipotesi previste dall'art. 8 (sicurezza pubblica, interessi finanziari statali, tutela dei diritti altrui e della ricerca scientifica e statistica) e che gli Stati, al fine del rispetto dei principi, si impegnano ad instaurare un sistema di ricorsi e sanzioni. Il carattere e il funzionamento degli stessi, a fronte del carattere non *self executing* della Convenzione, è tuttavia rimesso alla libera determinazione di questi ultimi.

In dottrina è stata manifestata qualche perplessità con riferimento alla scarsa incisività di alcune norme della Convenzione nonché alla latitudine concessa allo spazio di manovra degli Stati nell'attuazione dei principi di base[120]. Ciò sarebbe indicativo della cautela con cui gli Stati intendono assumere obblighi internazionali in materia. Cautela che trova conferma nella mancata previsione come, invece, auspicato dalla risoluzione 890 (80) dell'Assemblea consultiva del Consiglio d'Europa, di un meccanismo di controllo internazionale del rispetto degli obblighi convenzionali.

In ogni caso, ai fini della presente ricerca, occorre sottolineare come la Convenzione n. 108 del Consiglio d'Europa abbia introdotto per la prima volta il principio della protezione "equivalente", secondo il quale il trasferimento tra due Stati aderenti a tale Convenzione dei dati personali può avere luogo soltanto ove il sistema giuridico dello Stato destinatario del

[119] G. Cellamare, "*Tutela della vita privata e libera circolazione delle informazioni in una recente convenzione del Consiglio d'Europa*", in "*Rivista di Diritto Internazionale*", Anno 1982 Fascicolo 3 , pp 802 e ss.
[120] G. Cellamare, nota 119

flusso di informazioni garantisca il medesimo livello di tutela dello stato di origine. Tale principio verrà recepito anche successivamente dalla Direttiva 95/46/CE sulla protezione dei dati personali. L'espressione "equivalente" implica, dunque, un alto grado di compatibilità che costituisce di fatto un argine alla circolazione transfrontaliera dei dati personali[121]. Nella Convenzione 108, tuttavia, non è stato affrontato esplicitamente il tema del consenso[122] essendo la legittimazione al trattamento dei dati personali condizionata solamente all'adozione di "garanzie adatte" a tutela del soggetto cui i dati si riferiscono.

Successivamente alla stipula della Convenzione il Consiglio d'Europa è intervenuto con l'adozione di ben nove raccomandazione di carattere settoriale relative all'utilizzo dei dati personali da parte di svariate categorie di soggetti. In particolare con la raccomandazione R(89)2 del 18 gennaio 1989 è stata predisposta una disciplina di tutela dei dati personali in riferimento ai rapporti di lavoro; si è cercato così di ridurre al minimo i rischi che i metodi di elaborazione informatica dei dati utilizzati dai datori di lavoro potrebbero presentare per i diritti e le libertà dei lavoratori.

L'utilizza di uno strumento soft, ovvero privo di efficacia vincolante nei confronti dei Paesi dell'Unione, quale è la raccomandazione, ha impedito però che tale intervento potesse incidere concretamente sulle legislazioni interne. Ciò nonostante, sebbene il peso degli strumenti di soft law vada misurato soprattutto in termini politici anziché giuridici, occorre tenere a mente che gli stessi possono spesso costituire un primo nucleo di principi che in seguito possono evolversi in vere e proprie regole consuetudinarie o essere recepite in un trattato internazionale. Questo è il tipico caso di diverse dichiarazioni di principio dell'ONU che spesso hanno trovato riscontro in norme consuetudinarie o disposizioni pattizie.

Allo stesso modo, deve rammentarsi che, per quanto riguarda lo specifico ambito delle banche dati di polizia, la Raccomandazione 87(15) del Comitato dei Ministri del Consiglio d'Europa (che raccoglie i principi espressi dalla Convenzione 108) viene richiamata da alcune disposizioni della successiva Convenzione di Schengen del 1985. Tale richiamo rafforza perciò, il valore, almeno nell'area Schengen, di un atto di per sé non vincolante[123].

[121] Marco Botta e Mario Viola De Azevedo Cunha, nota 1

[122] Claudia Faleri, "*Autonomia Individuale e diritto alla riservatezza*", in "*Rivista Italiana di Diritto del Lavoro*" anno 2000 fascicolo 3, p. 305.

[123] Lucia Serena Rossi, "*La protezione dei dati personali negli accordi di Schengen alla luce degli standards fissati dal Consiglio d'Europa e dalla Comunità Europea*", in B. Nascimbene (a cura di) "*Da Schengen a Maastricht: "*, Milano 1995, pp. 163 e ss.

7. L'Unione Europea e l'affermazione dei diritti fondamentali nella giurisprudenza della Corte di Giustizia.

Come si è già detto in precedenza, la Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, entrata in vigore nel 1953 nel quadro dell'organizzazione del Consiglio d'Europa, ha rappresentato per molti anni a livello regionale europeo l'unico strumento internazionale contenente una specifica disposizione a tutela della privacy.

Diversamente, invece, la Comunità Economica Europea, istituita con il trattato di Roma del 1957 sulla scia dell'esperienza della Comunità Europea del Carbone e dell'Acciaio, è nata senza alcuna voce nel campo dei diritti fondamentali. Inizialmente, infatti, il suo scopo era unicamente quello di creare un mercato comune tra gli Stati membri caratterizzato dall'eliminazione dei dazi doganali, nonché degli ostacoli alla libera circolazione delle merci, dei lavoratori, dei servizi e dei capitali.

Fatti salvi alcuni principi generali da sempre incisi nel DNA storico del diritto comunitario, dunque (quali il principio di non discriminazione in base alla nazionalità), il Trattato istitutivo non conteneva alcun riferimento ai diritti fondamentali. Tale lacuna non era certo trascurabile in quanto l'ampiezza e l'intensità che hanno caratterizzato sin da subito l'azione della Comunità, ha fatto ben presto emergere il problema della sua incidenza sui principi fondamentali degli ordinamenti interni, in particolare quelli relativi alla tutela dei diritti dell'uomo.

Tutto questo, unitamente ad una vocazione puramente economica, nonché agli iniziali scarsi poteri del Parlamento Europeo di ingerirsi nel processo di adozione degli atti comunitari, ha contribuito ad alimentare le critiche rivolte per molto tempo alla Comunità in merito all'esistenza di un vero e proprio *deficit* democratico in seno al meccanismo di funzionamento delle sue istituzioni[124].

Per questo motivo il Parlamento Europeo, già nel 1989, manifestava l'esigenza di elaborare un catalogo comunitario dei diritti fondamentali[125] ed auspicava l'adesione della Comunità alla Convenzione Europea dei Diritti dell'Uomo[126]. Tale progetto veniva, tuttavia,

[124] Luigi Ferrari Bravo, Enzo Moavero Milanesi, "*Lezioni di Diritto Comunitario*", Napoli 2002, p. 17 e ss.

[125] Risoluzione del12 aprile 1989 con la quale è stata adottata la Dichiarazione dei diritti e delle libertà fondamentali in GUCE C 120/51 del 16 maggio 1989

[126] Si vedano le risoluzioni del 27 aprile 1979, del 9 luglio 1991, del 18 gennaio 1994 (GUCE C 44 del 14 febbraio 1994) del 17 maggio 1995 sul funzionamento dell'Unione europea (GUCE C 51 del 19 giugno 1995) e del 13 marzo 1996 in merito alla convocazione della CIG.

accantonato allorquando, come si vedrà più avanti, la Corte di Giustizia richiesta di un parere in merito, escludeva la competenza della Comunità ad aderire alla Convenzione senza una previa revisione dei Trattati istitutivi[127].

In particolare, sulle conseguenze di tale mancata adesione della Comunità alla CEDU si é registrato, in dottrina, un vivace dibattito. Secondo un primo, autorevole, orientamento[128] tale "inconveniente" non avrebbe affatto comportato problematiche di rilievo sotto il profilo della tutela dei diritti fondamentali. Invero, dopo quasi un cinquantennio di pronunce giurisprudenziali, non sarebbero rilevabili grosse divergenze con riguardo alla tutela dei diritti fondamentali da parte delle due Corti, considerato anche che in talune occasioni le stesse si sono pronunciate su casi analoghi.

Secondo un diverso orientamento[129], invece, la "conversione" della Corte di Giustizia alla protezione dei diritti fondamentali e in particolare quelli garantiti dalla CEDU non sarebbe stata totale, ma avrebbe lasciato sussistere, per diverso tempo, alcune sostanziali difformità tra la sua giurisprudenza e le decisioni degli organi del Consiglio d'Europa. In particolare, non sarebbero mancati i casi in cui la Corte di Giustizia avrebbe interpretato i diritti CEDU in chiave riduttiva e comunque assai diversa rispetto a quanto fatto dagli organi di Strasburgo.

A parere di chi scrive quest'ultimo orientamento risulta riflettere con maggiore realismo l'effettiva portata della giurisprudenza della Corte. Invero, come si vedrà compiutamente in prosieguo, dall'esame delle relative pronunce, emerge che la Corte di Giustizia non fa praticamente mai rinvio ai principi CEDU in quanto tali. Al contrario essa quasi sempre li trasforma in principi generali del diritto comunitario, interpretandoli alla luce dei propri paradigmi e dei propri precedenti. Allo stesso modo, giova evidenziare il fatto che la Corte si riserva, altresì, di privilegiare in ultima analisi valori essenziali del diritto comunitario rispetto alla protezione dei diritti individuali. In quest'ottica, l'esistenza delle suesposte divergenze nell'interpretazione e nell'applicazione dei diritti fondamentali da parte della giurisprudenza delle due corti appare difficilmente negabile.

In ogni caso, ferme restando le considerazioni che precedono, appare comunque fondata l'opinione di chi ritiene che la giurisprudenza della Corte di Giustizia sia stata in grado di compensare, almeno in parte, tanto la mancanza di una disposizione materiale nel Trattato sui diritti fondamentali, quanto la circostanza della mancata adesione della Comunità

[127] Parere n. 2/94 del 26 marzo 1996 in Raccolta I - 1763
[128] Giuseppe Tesauro, "*Diritto Comunitario*", Padova 2003, p. 130 e ss.
[129] Lucia Serena Rossi, "*Il parere 2/94 sull'adesione della Comunità Europea alla Convenzione Europea dei Diritti dell'Uomo"* in Diritto dell'Unione Europea, 1996 fasc. 3 p. 839

alla Convenzione Europea per i diritti dell'Uomo di Strasburgo[130]. A ben vedere, infatti, se si considera che i "progressi" raggiunti dalla giurisprudenza della Corte di Giustizia non sono mai stati accompagnati da analoghi sforzi da parte dei Trattati[131] (i quali, anzi, si sono spesso limitati a "codificare" i principi enucleati dalle decisioni della Corte[132]) sembra cogliere nel segno l'affermazione di chi ha evidenziato che, grazie al lavoro interpretativo della Corte di Giustizia, la CEDU sia stata in qualche modo "comunitarizzata", senza che la Comunità sia mai divenuta parte della stessa[133].

Ciò premesso, come si accennava in precedenza, nell'iniziale silenzio dei Trattati l'impegno a garantire i diritti fondamentali è stato assunto, dopo un periodo di agnosticismo, proprio dalla Corte di Giustizia.

In una prima fase, infatti, la Corte aveva assunto una posizione astensionista, escludendo che potesse rientrare tra i propri compiti quello di garantire il rispetto dei diritti posti a tutela degli individui negli ordinamenti interni, ad essa incombendo solo di assicurare il rispetto del diritto nell'interpretazione e nell'applicazione del diritto comunitario[134]. In seguito, dopo una iniziale diffidenza volta a preservare il diritto comunitario da incursioni di valori all'epoca considerati esterni, la Corte di Giustizia è passata a posizioni dichiaratamente garantistiche[135].

Con la sentenza *Stauder* del 12 novembre 1969[136], infatti, la Corte ha affermato, sia pure incidentalmente, il principio per cui i diritti fondamentali della persona formano parte del diritto comunitario in quanto principi generali, consacrandone così l'ingresso nel relativo sistema delle fonti.

---

[130] Giuseppe Tesauro, nota 128

[131] In particolare, la clausola del trattato di Maastricht del 7 febbraio 1992 sull'impegno dell'Unione a rispettare i diritti fondamentali "*quali risultano dalle tradizioni costituzionali comuni degli Stati membri, in quanto principi generali del diritto comunitario*" (art. F, al. 2), si limita a codificare un indirizzo consolidato della giurisprudenza comunitaria. Non solo, ma anche la successiva Carta dei diritti fondamentali dell'Unione, solennemente proclamata il 7 dicembre 2000 al vertice di Nizza, può considerarsi ricognitiva di un complesso di diritti enucleati dalle tradizioni costituzionali comuni nella paziente opera interpretativa della Corte di giustizia.

[133] Maria Rosaria Donnarumma, "Il *processo di costituzionalizzazione dell'Unione Europea e la tensione dialettica tra la giurisprudenza della Corte di Giustizia e le giurisprudenze delle corti costituzionali*", in Riv. it. dir. pubbl. comunit. 2010, 02, 407

[134] Causa C-1/58 Stork, sentenza del 4 febbraio 1959 in Raccolta 17; Cause C-36-38 e 40/59, Uffici di vendita del Carbone della Ruhr, sentenza del 15 luglio 1960 in Raccolta 423; Causa C-40/64 Sgarlata, sentenza del 1 aprile 1965, in Raccolta 227.

[135] Cfr. Lucia Serena Rossi, cit. sub nota 123 supra

[136] Cfr. Causa C-26/69 Erich Stauder contro Città di Ulm-Sozialamt, in Raccolta, 1970, 419

Tale principio è divenuto parte integrante della giurisprudenza consolidata della Corte di Giustizia ed è stato successivamente affermato anche in altre importanti pronunce[137]. Tuttavia, a questo stadio embrionale della giurisprudenza della Corte, restava aperta la questione della concreta individuazione dei diritti fondamentali, nonché quello della determinazione della loro rilevanza a livello comunitario. Parimenti, le pronunce iniziali non affrontavano neppure la questione dell'armonizzazione di tali principi generali con quelli riconosciuti dagli Stati membri.

Un significativo tentativo di precisazione della portata della giurisprudenza *Stauder* si è avuto con la sentenza *Internationale Handelsgesellschaft* del 17 dicembre 1970[138]. In questa seconda fase la Corte, sollecitata dalla giurisprudenza delle Corti costituzionali tedesca[139] ed italiana[140], ha utilizzato la protezione dei diritti umani quale vero e proprio strumento di integrazione europea[141], affermando che la "*salvaguardia dei diritti fondamentali, pur essendo informata alle tradizioni costituzionali comuni agli Stati membri, va garantita entro l'ambito della struttura e delle finalità della Comunità*".

Mediante questa pronunci, pertanto, la Corte ha ribadito la propria intenzione di assicurare la protezione dei diritti fondamentali derivanti dalle tradizioni costituzionali comuni degli Stati membri precisando, tuttavia, come la relativa fonte di legittimazione debba essere individuata esclusivamente nei principi generali del diritto comunitario, intesi quale fonte autonoma dell'ordinamento europeo. In altre parole, secondo la Corte, tali diritti fondamentali vengono in rilievo soltanto nei limiti della loro compatibilità con la struttura e con le finalità delle Comunità.

Secondo autorevole dottrina[142] questo inciso risolverebbe l'apparente contraddizione con l'altra affermazione contenuta nella stessa decisione (e in altre successive) per cui l'eventuale contrasto di un atto comunitario con norme anche costituzionali di uno stato membro, anche se relative ai diritti fondamentali, non può inficiare la sua validità né la sua efficacia nel territorio dello Stato stesso pena l'efficacia e l'unità del diritto comunitario.

---

[137] Cfr. *Ex plurimis* Causa C-5/88, Wachauf, sentenza del 13 luglio 1989 in Raccolta 2609; Causa C-274/99 Connoly, sentenza del 6 marzo 2001 in Raccolta I-1611; Causa C-94/00 Roquette Frères S.A., sentenza del 22 ottobre 2002, in Raccolta I-9011.

[138] Cfr. Causa C-11/70 Internationale Handelsgesellschaft Mbh contro Einfuhrund Vorratsstelle fuer getreide und futtermittel, in Raccolta, 1970, 1125, par. 4.

[139] Le principali sentenze sono: Corte costituzionale federale, sentenza 29 maggio 1974 (Solange I); sentenza 22 ottobre 1986 (Solange II); ordinanza 12 maggio 1989; sentenza 12 ottobre 1993.

[140] Le principali sentenze sono in particolare, Corte costituzionale, sentenza 27 dicembre 1965, n. 98; sentenza 27 dicembre 1973, n. 183 (Frontini); sentenza 8 giugno 1984, n. 170 (Granital); sentenza 21 aprile 1989, n. 232 (Fragd).

[141] Chiti Edoardo, "*La tutela dei diritti dell'uomo nell'ordinamento comunitario*", in Giornale Dir. Amm., 1996, 10, 959

[142] Girolamo Strozzi, "Diritto dell'Unione Europea, Parte Istituzionale", Terza Edizione Torino 2005 p. 250

Successivamente, nella sentenza Nold del 14 maggio 1974[143], la Corte di Giustizia ha indicato per la prima volta, tra le fonti di ispirazione dei principi generali del diritto comunitario in materia di diritti fondamentali, anche gli strumenti internazionali relativi alla tutela dei diritti umani. Nella fattispecie la Corte ha affermato che "*i trattati internazionali relativi alla tutela dei diritti dell'uomo cui gli Stati membri hanno cooperato o aderito possono del pari fornire elementi di cui occorre tenere conto nell'ambito del diritto comunitario".* Inoltre, nella sentenza *Nold* é apparso maggiormente accentuato l'impegno della Corte di assicurare la protezione dei diritti fondamentali, sia perché in questa pronuncia la stessa si è detta propriamente "vincolata" alle tradizioni costituzionali comuni, sia perché ha affermato di non poter ammettere provvedimenti incompatibili con i diritti fondamentali riconosciuti e garantiti dalle costituzioni degli Stati membri.

In ogni caso, tra tutti i trattati internazionali a cui la Corte ha dichiarato di ispirarsi, il più importante è certamente la Convenzione europea dei diritti dell'uomo, che la Corte cita per la prima volta nel 1975[144], ed in numerosi casi successivi.

In questa sede giova, comunque, importante sottolineare che, nell'ottica della Corte, i richiami agli strumenti internazionali e alla CEDU non comportano affatto l'incorporazione automatica dei diritti ivi previsti nel diritto comunitario. Al contrario, essa traccia dei limiti ben precisi a tale operazione, subordinando la tutela dei diritti fondamentali alla loro compatibilità con i principi essenziali e con le finalità dell'ordinamento comunitario. In altri termini, come è stato rilevato in dottrina[145], la Corte si riserva la prerogativa di "selezionare" i diritti fondamentali che intende incorporare e tutelare nell'ordinamento comunitario in ragione della loro armonizzazione con i fondamenti del sistema europeo ed in pari tempo collocare la loro protezione ad un livello inferiore rispetto ai Trattati istitutivi laddove questi risultino non conformi al sistema comunitario o quando risultino pregiudicare il perseguimento delle relative finalità. Sentenze quali *Hauer o Grogan* esemplificano la disinvoltura della Corte nel subordinare il riconoscimento di un certo diritto quale diritto fondamentale comunitario al raggiungimento dell'obiettivo, prioritario, dell'effettività del diritto comunitario[146].

Ciò premesso, una significativa svolta nella giurisprudenza della Corte, contenente un importante rinvio ai criteri interpretativi utilizzati dalla Corte di Strasburgo per la rilevazione

[143] Nold c. Commissione delle Comunità europee, Causa 4/73, in Raccolta, 1974, 491.
[144] Rutili c. Ministre de l'Interieur, Causa 36/75, in Raccolta, 1975, 1219
[145] R. Adam, A. Tizzano, "Lineamenti di Diritto dell'Unione Europea", Torino 2007, p. 122 e ss.
[146] The Society for the Protection of Unborn Children (Ireland) Ltd. c. Grogan, Causa C-159/90, in Raccolta, 1991, 4685

dei diritti fondamentali si è avuta con il caso Bausthahlgewebe[147]. Tale caso ha avuto ad oggetto la presentazione alla Corte di giustizia di una impugnazione avverso una sentenza del Tribunale di primo grado fondata sulla presunta violazione dell'art. 6 della Convenzione Europea dei Diritti dell'Uomo in ragione dell'eccessiva durata della procedura.

L'avvocato generale, dal canto suo, si è pronunciato in favore della ricevibilità di tale motivo di ricorso[148], argomentando che negare alla Corte il dovere di controllare l'applicazione corretta dell'art. 6 TUE da parte del Tribunale implicherebbe dover ammettere che esso non è soggetto al suo rispetto, mentre tale articolo sancisce l'impegno dell'Unione a rispettare i diritti fondamentali quali garantiti dalla Convenzione Europea e dunque il dovere della Corte di assicurarne l'osservanza.

Ciò premesso, nella sentenza *Baustahlgewebe* la Corte ha affermato il principio generale di diritto comunitario in forza del quale ciascuna persona ha diritto ad un processo equo che si ispira ai principi fondamentali consacrati dalla CEDU, ed in particolare il diritto ad un processo entro un termine ragionevole.

Più specificamente la Corte ha affermato che "l*'art. 6 n. 1 CEDU di dispone che ogni persona ha diritto ad un'equa pubblica udienza entro un termine ragionevole, davanti ad un tribunale indipendente ed imparziale istituito per legge, al fine della determinazione sia dei suoi diritti e dei suoi doveri di carattere civile, sia della fondatezza di ogni accusa penale che le venga rivolta. Il principio generale di diritto comunitario in forza del quale ogni persona ha diritto ad un processo equo che si ispira a tali diritti fondamentali (…) e in particolare il diritto ad un processo entro un termine ragionevole si applica nell'ambito di un ricorso giurisdizionale avverso una decisione della Commissione che infligge ammende a un'impresa per violazione del diritto della concorrenza*[149]:"

In ogni caso la Corte ha, comunque, precisato che la ragionevolezza della durata di un procedimento non può essere desunta soltanto sulla base della mera durata del medesimo, dovendo essere valutata in concreto alla luce delle circostanze proprie di ciascuna causa e in particolare della rilevanza della lite per l'interessato, della complessità della causa, nonché del comportamento del ricorrente e di quello delle autorità competenti .[150] A questo proposito la Corte vieppiù afferma che la ragionevolezza della durata della procedura innanzi al Tribunale deve essere valutata in analogia con quanto emerge dalla giurisprudenza della Corte europea in materia.

[147] Causa C-185/95 P Baustahlgewebe GmbH c. Commissione, sentenza del 17 novembre 1998 in Raccolta I-8417
[148] Causa C- C-185/95 P Baustahlgewebe GmbH c. Commissione, Conclusioni dell'Avvocato Generale Jacobs
[149] V. punti 20-21 della sentenza Bausthahlgewebe c. Commissione cit.
[150] V. punto 29 della sentenza Bausthahlgewebe c. Commissione cit.

Questa presa di posizione della Corte di Giustizia in materia di diritti fondamentali ha formato oggetto di particolare attenzione da parte della dottrina[151] la quale non ha mancato di osservare come la Corte sia passata dall'affermazione di quel "significato particolare" rivestito dalla CEDU nell'ambito dei trattati internazionali in materia di diritti dell'uomo ai quali l'ordinamento comunitario si ispira per la tutela dei diritti fondamentali, ad un richiamo esplicito e puntuale alla giurisprudenza della Corte Europea per i diritti dell'uomo.

In ogni caso, durante il corso degli anni la giurisprudenza della Corte di Giustizia ha riconosciuto numerosi diritti fondamentali di cui assicura il rispetto nell'ordinamento comunitario, sebbene alle condizioni da essa di volta in volta fissate:

- uguaglianza e non discriminazione[152]

- libertà di religione[153]

- libertà di espressione e di informazione[154]

- libertà di circolazione ed associazione[155]

- inviolabilità del domicilio[156] (che tuttavia non può essere invocata per tutelare l'inviolabilità dei locali commerciali[157])

- diritto di proprietà, che può tuttavia incontrare dei limiti in funzione dell'interesse generale[158]

- diritto ad una tutela giurisdizionale effettiva[159]

- diritto ad un giusto processo[160] che implica anche la sua non eccessiva durata[161]

- non retroattività delle norme penali e rispetto dei diritti della difesa[162], (sotto riserva della retroattività della legge penale più favorevole)

- non discriminazione in ragione del sesso[163]

---

[151] Pietro Manzini, *"Sull'irragionevole durata delle procedure comunitarie"*, in Diritto dell'Unione Europea, 1999, 3 p. 511

[152] Causa C-41/84 Pinna, sentenza del 15 gennaio 1986 in Raccolta, 1; Causa C- 174/89, Firma Hoche, sentenza del 28 giugno 1990 in Raccolta 2681; Causa C-158/97 Badeck, sentenza del 28 marzo 2000 in Raccolta I-1875;

[153] Causa C-130/75 Prais, sentenza del 27 ottobre 1976, in Raccolta, 1589

[154] cfr ex plurimis Causa C-100/88 Oyowe, sentenza del 13 dicembre 1989 in Raccolta 4285; Causa C-260/89 ERT, sentenza del 18 giugno 1991 in Raccolta I-2925; Causa C-288/89 Gouda, sentenza del 25 luglio 1991, in Raccolta I-4007

[155] cfr. ex plurimis Causa C-18/74 Syndicat Général, sentenza del 8 ottobre 1974 in Raccolta 933; Causa C-36/75 Rutili, sentenza del 28 ottobre 1975 in Raccolta 1219

[156] Cause C-46/87 e C-227/88 Hoechst, sentenza del 21 settembre 1989, in Raccolta 2859

[157] Cause C- 97 e 99/89 Dow Chemical Iberia , sentenza del 17 ottobre 1989, in Raccolta 3165

[158] Causa C-44/79, Hauer, sentenza del 13 dicembre 1979, in Raccolta 3727, Cause C-41,121, e 796/79 Testa, sentenza del 19 giugno 1980, in Raccolta 1979, Causa C-234/85 Franz Keller, sentenza del 8 ottobre 1986, in Raccolta 2897

[159] Causa C-222/84, Johnston, sentenza del 15 maggio 1986, in raccolta 1651; Causa C-340/89 Vlassopoulou, sentenza del 7 maggio 1991 in Raccolta 2357; Causa C-87-89/90 Verholem, sentenza del 11 luglio 1991 in Raccolta 3757

[160] Causa C-209-215/78 Van Landeweyck, sentenza del 29 ottobre 1980 in Raccolta 3125; Causa 100-103/80 Musique Diffusion sentenza del 7 giugno 1983; in raccolta 1825;

[161] Causa C -85/98 Bausthahlgewebe, sentenza del 17 dicembre 1998, in Raccolta I-8417

[162] Causa C-63/83 Kent Kirk sentenza del 19 luglio 1984 in Raccolta 2689;

E' stato, inoltre, riconosciuto anche il diritto al pluralismo dell'informazione, nonché il diritto ad una buona amministrazione. E' appena il caso di notare che l'esercizio dei diritti fondamentali può essere oggetto di restrizioni in vista di obiettivi di interesse generale perseguiti dalla Comunità[164]

8. Il case law della Corte di Giustizia in materia di tutela dei dati personali

La giurisprudenza della Corte di Giustizia si é confrontata più volte con il tema della protezione dei dati personali. Esiste, infatti, un numero assai nutrito di pronunce della Corte in questa materia, a conferma del fatto che, per l'ordinamento giuridico dell'Unione Europea, la tutela dei dati rappresenta, oggi, un vero e proprio diritto fondamentale dell'individuo.

Tale diritto ha fatto la propria comparsa nell'ordinamento giuridico dell'Unione in epoca piuttosto recente, a seguito del progresso della tecnologia e dell'uso generalizzato dei computer. Alla sua attuale definizione in ambito europeo ha contribuito in larga misura proprio l'elaborazione giurisprudenziale ad opera della Corte di Giustizia, rendendolo così un tipico caso di diritto fondamentale nato in via pretoria, prima ancora di essere positivizzato.

Le decisioni della Corte di Giustizia in questa materia seguono in buona parte il solco già tracciato dalle pronunce della Corte Europea dei Diritti dell'Uomo sulla base della CEDU e degli altri strumenti internazionali vigenti nel quadro del Consiglio d'Europa. Come opportunamente osservato dall'Avvocato Generale Sharpston nelle conclusioni presentate nell'ambito della causa Bavarian Lager[165], infatti, la Convenzione 108 del Consiglio d'Europa sul trattamento automatizzato dei dati ha funto, da "*precursore della tutela di questo aspetto della vita privata, entrando nell'ordinamento comunitario attraverso le tradizioni costituzionali comuni degli Stati membri*"[166].

La giurisprudenza della Corte di Giustizia in materia di tutela dei dati personali si è venuta, così, ad inserire nell'ambito di un "sistema di protezione multilivello", che caratterizza attualmente la situazione di tutti diritti fondamentali in Europa e che "*si contraddistingue per la molteplicità delle fonti di riconoscimento dei diritti e dell'estensione*

[163] Causa C-80/70, Defrenne, sentenza del 25 maggio 1971
[164] Wachauf ; Bosphorus causa C- 84/95 sentenza 30 luglio 1996 in Raccolta 3953
[165] Cfr. punto 100 delle conclusioni dell'Avvocato Generale Eleanor Sharpston nella causa C-28/08 Bavarian Lager c. Commissione.
[166] Sebbene, in realtà, prima dell'intervento del Legislatore europeo l'esistenza di una tradizione costituzionale comune degli Stati membri in materia di tutela dei dati è difficilmente ravvisabile.

dei relativi ambiti di tutela, come garantiti nel "diritto vivente" scaturente dalle diverse autorità giudiziarie chiamate ad inverarli: Corti Costituzionali, Corte di Strasburgo e Corte di Giustizia[167]".

Ciò premesso, ad avviso di chi scrive, sebbene sia innegabile che la tutela dei dati personali nell'ambito dell'ordinamento giuridico dell'Unione Europea sia largamente tributaria dell'esperienza degli organi del Consiglio d'Europa, l'analisi delle decisioni della Corte di Giustizia in questa delicata materia consente di cogliere alcune significative distinzioni.

E' stato, innanzitutto, osservato[168] come il ruolo della Corte di Strasburgo sia quello di tutelare e bilanciare tra loro unicamente i diritti fondamentali. Conseguentemente le sue pronunce si caratterizzano per avere un taglio ed un tono prettamente costituzionale difficilmente rilevabile nelle pronunce della Corte di Giustizia, la quale deve invece tenere conto anche dei principi dell'economia e del libero mercato. Secondo questa parte della dottrina, dunque, la Corte di Strasburgo sarebbe la Corte dei Diritti laddove, invece, la Corte di Giustizia rimarrebbe piuttosto un giudice delle libertà economiche. In realtà, secondo altri osservatori[169] non sono mancate pronunce[170] in cui la Corte di Giustizia ha svolto anch'essa un'operazione interpretativa analoga a quella di una corte costituzionale, utilizzando tecniche di giudizio proprie del controllo di costituzionalità e ricoprendo, così, il ruolo di garante ultimo della proporzionalità delle norme non soltanto rispetto alla Corte di Strasburgo, ma anche alle corti costituzionali nazionali.

In secondo luogo, mentre nel panorama della CEDU e della relativa giurisprudenza la tutela dei dati personali viene concepita come un aspetto del più ampio diritto al rispetto alla vita privata e familiare, nell'ordinamento giuridico europeo tale diritto viene ad assumere, con il passare degli anni, una valenza autonoma. In particolare, la copiosa attività giurisprudenziale della Corte di Giustizia ha, senza dubbio, incoraggiato la sua codificazione all'art. 8 della Carta dei Diritti Fondamentali dell'Unione Europea[171] e ciò in una disposizione separata in relazione al diritto al rispetto della vita privata (art. 7) e a quella famigliare (art. 9). A differenza dell'art. 8 CEDU, dunque, la tutela in tre specifici articoli ha permesso di recepire, nel diritto primario dell'Unione Europea, la decennale giurisprudenza della Corte di

[167] Giulia Tiberi, "*Il diritto alla protezione dei dati personali nelle carte e nelle corti sovranazionali*", in Cassazione Penale, 2009, 11, p. 4667 e ss.
[168] Mario Cartabia, "*Principi inviolabili e integrazione europea*", Milano, 1995 pag. 134 e ss..
[169] Denicolò-Palermo "*La riservatezza….senza riserve*", in *Diritto Pubblico Comparato ed europeo*, 2003, p. 1255 e ss.
[170] Cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e a., sentenza del 20 maggio 2003
[171] Proclamata solennemente il 7 dicembre 2000 dal Parlamento europeo, dal Consiglio e dalla Commissione (GU C 364, pag. 1 e segg.)

Strasburgo per adattarla ad una società in costante evoluzione sotto il profilo sociale, economico e culturale.

Peraltro, il Trattato di Lisbona, oltre ad aver contemplato l'inserimento della tutela dei dati personali all'art. 16 del TFUE, ha da ultimo conferito alla Carta dei Diritti Fondamentali il medesimo valore giuridico dei trattati superando, così, ogni incertezza in merito alla natura cogente delle sue disposizioni, la valenza delle quali ha, invece, in epoca anteriore, notoriamente attraversato un periodo di incertezza applicativa in ragione della sua condizione di atto di *soft law*[172].

Allo stesso modo, se la prima stagione delle pronunce della Corte di Giustizia in materia di tutela dei dati e della vita privata si é caratterizzata per il suo ampio rinvio alle disposizioni della CEDU ed alle decisioni della Corte Europea dei Diritti dell'Uomo, in epoca più recente la Corte pare maggiormente orientata verso l'utilizzo di criteri di rilevazione e di apprezzamento propri, mutuati direttamente dall'ordinamento giuridico europeo, che essa impiega anche allorquando si trova a sindacare la legittimità di ogni restrizione dei diritti fondamentali.

Invero, la Corte di Giustizia non si è mai limitata a trarre semplicemente "ispirazione" dalla giurisprudenza della Corte di Strasburgo in materia di protezione dei dati personali, ma ha proceduto ad incorporarla direttamente nelle proprie decisioni. Ma questo è avvenuto senza che la Corte abbia mai menzionato mai né la clausola di corrispondenza prevista dalla carta di Nizza all'art. 52 par. 3 né la clausola sul livello di protezione di cui all'art. 53 della Carta, evitando anzi accuratamente di confrontare le deroghe previste dalla direttiva per giustificare l'ingerenza nella vita privata con le ipotesi previste dalla CEDU. In questo modo la ha preservato la propria libertà, in casi futuri, di giungere ad un bilanciamento diverso rispetto a quello operato dalla Corte di Strasburgo, qualora dovesse rilevare una portata del diritto tutelata a livello comunitario diversa da quella garantita nel sistema CEDU[173].

Non mancano, inoltre, sentenze della Corte di Giustizia in materia di tutela dei dati personali in cui, a dispetto dell'espresso invito in tal senso contenuto nelle conclusioni degli avvocati generali[174], qualsiasi riferimento alla CEDU risulta del tutto assente[175]. In altri termini la Corte di Giustizia sembra, con il passare degli anni, aver raffinato una propria autonoma giurisprudenza, con la conseguenza che, attualmente, la stessa non si limita più

[172] v. punto 22 delle conclusioni dell'Avvocato Generale Damaso Ruiz Arabo Colomer nella causa C-553/07 College Van Burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer
[173] Giulia Tiberi, cit. sub nota 167
[174] V. punto 37 delle conclusioni dell'Avvocato Generale Juliane Kokott nella causa C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinaporssi
[175] cfr. ex plurimis causa C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinaporssi, sentenza del 13 dicembre 2008

semplicemente ad applicare i criteri mutuati dalla giurisprudenza CEDU, optando per un sempre maggiore ricorso a criteri di valutazione suoi propri, elaborati a partire dal diritto dell'Unione.

Come si accennava poc'anzi la giurisprudenza della Corte di Giustizia in materia di dati personali ha registrato una costante evoluzione nel corso degli anni, ed ha puntualmente preceduto tutti gli interventi di codificazione da parte del legislatore europeo il quale ha, di fatto, mutuato dalle decisioni della Corte numerosi dei principi accolti successivamente dalla normativa comunitaria. Guardando più da vicino al trend dell'evoluzione giurisprudenziale è possibile suddividere il percorso seguito dall'orientamento della Corte in almeno tre fasi.

In un primo momento, infatti, a partire dalla remota sentenza *Stauder*[176], la giurisprudenza della Corte di Giustizia ha inquadrato la tutela della vita privata tra i principi generali del diritto comunitario, operando poco tempo dopo tale inserimento in relazione all'esame dell'adempimento dell'obbligo di fornire dati, come il nome[177] o le informazioni sanitarie[178] sia sul piano nazionale[179] che comunitario[180]. In particolare, con la giurisprudenza inaugurata nella causa *National Panasonic*[181], la Corte ha esteso anche alle persone giuridiche la tutela tradizionalmente accordata dai diritti fondamentali ai dati personali, al domicilio ed alla corrispondenza degli individui.

Successivamente, specie nel corso della prima metà degli anni novanta, la Corte di giustizia ha affermato l'incidenza del diritto alla tutela dei dati nell'ambito della vita privata[182] e familiare[183], iniziando a riconoscere l'invocabilità dell'art. 8 CEDU in relazione alla protezione dei dati personali e a richiamare la giurisprudenza della Corte di Strasburgo in materia, utilizzando come criteri di giudizio gli stessi requisiti che in nome della CEDU possono giustificare un'ingerenza nella vita privata (previsione con legge, necessità in una società democratica, perseguimento di uno scopo legittimo). In questa fase, che vede la luce nell'ambito delle vertenze promosse dal personale delle istituzioni comunitarie, la Corte non

[176] Causa C-29/69 Stauder Sentenza del 12 novembre 1969, (Racc. pag. 419, punto 7)
[177] Causa C- 145/83, Adams/Commissione Sentenza 7 novembre 1985, (Racc. pag. 3539, punto 34)
[178] Sentenza 7 ottobre 1987, causa 140/86, Strack/Commissione (Racc. pag. 3939, punti 9-11)
[179] Sentenza 8 aprile 1992, causa C-62/90, Commissione/Germania (Racc. pag. I-2575, punto 23)
[180] Sentenza 5 ottobre 1994, causa C-404/92 P, X/Commissione (Racc. pag. I-4737, punti 17 e 18)
[181] Causa C-136/79 National Panasonic Limited c. Commissione, sentenza del 26 giugno 1980 in Racc. 2057. Orientamento confermato nella causa C-94/00 Roquette Frères S.A., sentenza del 22 ottobre 2002, in Raccolta I-9011. La sua giurisprudenza precedente, invero, era di segno contrario. Si veda cause riunite C-46/87 e C-227/88 Hoechst, sentenza del 21 settembre 1989, in Raccolta 2859
[182] Sentenze 21 settembre 1989, cause riunite 46/87 e 227/88, Hoechst/Commissione (Racc. pag. 2859), e 22 ottobre 2002, causa C-94/00, Roquette Frères (Racc. pag. I-9011)
[183] Sentenze 11 luglio 2002, causa C-60/00, Carpenter (Racc. pag. I-6279, punto 38), e 25 luglio 2002, causa C-459/99, MRAX (Racc. pag. I-6591, punto 53)

si è limitata a censurare la creazione di dossier segreti sui funzionari[184], ma si è espressa altresì per la necessità di proteggere il trattamento dei dati riguardante la salute degli interessati, riconoscendo che "*il diritto al rispetto della sfera privata e alla tutela del segreto medico, che ne è uno degli aspetti, costituiscono diritti fondamentali tutelati dall'ordinamento giuridico comunitario*[185]" che patiscono restrizioni solo se assolutamente indispensabili a tutelare obiettivi di interesse generali.

Ma è soltanto a partire dall'epoca successiva al 1996, anno di entrata in vigore della celebre direttiva n. 95/46 sulla protezione dei dati personali, che la giurisprudenza della Corte, fino a quel momento sporadica e casistica, ha trovato un bastione più solido per le proprie decisioni.

Infatti, la sentenza Österreichischer Rundfunk[186] ha confermato che la direttiva 95/46, pur avendo come obiettivo principale quello di garantire la libera circolazione dei dati personali, svolge altresì un'importante funzione a garanzia dei diritti fondamentali. E', interessante notare che, con tale pronuncia, la Corte si è discostata vistosamente dalle conclusioni dell'Avvocato Generale Tizzano, per le quali la salvaguardia dei diritti fondamentali, ivi compresa la tutela dei dati personali, pur rappresentando un importante valore di cui il legislatore comunitario ha tenuto conto nel delineare la disciplina di armonizzazione necessaria per l'instaurazione ed il funzionamento del mercato interno, non costituirebbe *"un autonomo obiettivo della direttiva"*[187].

In realtà la Giurisprudenza della Corte ha dimostrato a più riprese di essere giunta a conclusioni assai diverse. Nella causa *College van Burgemeester*[188], la Corte ha affermato proprio come la protezione dei diritti fondamentali rientri tra gli obiettivi della direttiva n. 95/46 sulla protezione dei dati personali[189]. Tale presa di posizione risulta indirettamente confermata anche nella sentenza relativa alla causa *Commissione c. Germania* del 2007[190], in cui la Grande Sezione della Corte di Giustizia ha stabilito che le autorità di controllo competenti per la sorveglianza del trattamento dei dati personali da parte degli organismi diversi da quelli pubblici e delle imprese di diritto pubblico che partecipano alla concorrenza sul mercato devono essere pienamente indipendenti.

---

[184] Causa T-39/93 e T-553/93 Baltasavias c. Commissione, sentenza del 11 ottobre 1995
[185] Sentenza relativa alla causa Commissione c. Germania cit. sub nota n. 169
[186] V. Cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk cit. sub nota 162
[187] v. punto 53 delle conclusioni dell'Avvocato Generale Antonio Tizzano in cause riunite C-465/00, C-138/01 e C-139/01, Österreichischer Rundfunk e a. (Racc. *pagina I-04989)*
[188] C-553/07, College van Burgemeester van Rotterdam c/ Rijkeboer, sentenza del 7 maggio 2009
[189] Nonostante si sia registrato un leggero passo indietro nella precedente causa Lindqvist
[190] Causa C-518/07 Commissione c. Germania, sentenza del 15 marzo 2010

In questo modo ha affermato che la Germania, sottoponendo dette autorità alla vigilanza dello Stato nei vari Länder, non aveva correttamente trasposto la direttiva 95/46 con riferimento all'art. 28. Tale arresto giurisprudenziale ha, secondo la dottrina più attenta[191], spianato la strada ad una concezione propriamente europea di indipendenza delle autorità poste a garanzia della tutela dei dati, e ciò proprio in chiave di una maggiore protezione dei diritti fondamentali dei cittadini dell'Unione[192].

In epoca ultima, invece, la Corte, dopo aver attraversato un periodo in cui il proprio orientamento era diretto ad affermare l'importanza della tutela dei diritti fondamentali nell'ambito dell'ordinamento giuridico dell'Unione ed a precisare l'ambito di applicazione della direttiva sulla protezione dei dati, si è occupata della delicata questione del bilanciamento oltre che della sincronizzazione di tale diritto con altri diritti fondamentali.

In questa fase si può rilevare come la giurisprudenza della Corte sviluppi un approccio prettamente casistico. Tuttavia, si deve altresì evidenziare come quest'ultima stagione delle pronunce della Corte non sia priva di incertezze. In alcune decisioni, infatti, (segnatamente nella causa *Bavarian Lager*) è parso di cogliere la volontà della Corte di conferire alla tutela dei dati un valore preponderante anche rispetto ad altri diritti di pari rango, laddove in altre pronunce (in particolare la sentenza *Promusicae*) la tutela dei dati personali sembra arretrare di fronte ad altri diritti fondamentali, quali la proprietà intellettuale.

Come osservato anche dall'Avvocato Generale Juliane Kokott nelle conclusioni rassegnate nella causa Tietosuojavaltuutettu c. Satakunnan Markkinaporssi[193], infatti, la Corte di giustizia è stata "*molto reticente nel determinare la portata della tutela dei dati e nel ponderare diritti fondamentali contrastanti. Nella sentenza Promusicae, essa si è limitata a menzionare i due diritti fondamentali ed a lasciare al giudice del rinvio il loro bilanciamento vero e proprio*" laddove *"nella sentenza Österreichischer Rundfunk e a. procedeva in modo analogo, fornendo tuttavia in aggiunta alcune indicazioni al giudice del rinvio*".

In ogni caso, nell'ottica di chi scrive la prudenza manifestata dalla Corte di Giustizia nelle operazioni di bilanciamento tra diritti fondamentali di pari rango è stata comunque opportuna, tenuto altresì conto che il suo ruolo, in sede di rinvio pregiudiziale, non è quello di sostituirsi al giudice nazionale nello statuire sulla controversia, bensì più propriamente quello di fornire a quest'ultimo "*risposte utili, ed in particolare fornire indicazioni, ricavate dal fascicolo*

[191] Fabienne Kauff-Gazin, "*Vers une conception de l'independence des autorités de régulation ? A propos de l'affaire C-518/07 Commission c. Allemagne* », in Europe n° 7, Juillet 2010, étude 9
[192] Causa C-518/07, punto 24 della decisione.
[193] Cfr. punti 46 e ss. delle conclusioni dell'Avvocato Generale Juliane Kokott nell'ambito della causa C-73/07, Tietosuojavaltuutettu c. Satakunnan Markkinaporssi.

della causa principale nonché dalle osservazioni scritte e orali ad essa sottoposte, che consentano a tale giudice di pronunciarsi sulla concreta controversia ad esso sottoposta"[194].

Ovviamente, ciò non significa che la Corte non sia capace di emettere decisioni suscettibili di incidere, anche profondamente, sugli interessi in gioco. Infatti, nonostante il rinvio pregiudiziale non attribuisca alla Corte di Giustizia la competenza a sindacare il diritto interno dei Paesi membri, fin dal caso *Van Gend en Loos* del 1962, la Corte ha sempre affermato la propria competenza, non solo ad interpretare il diritto comunitario, ma anche ad interpretare il quesito sottopostole dal giudice del rinvio, integrandone e colmandone le eventuali lacune. Attraverso l'interpretazione della domanda e l'integrazione del quesito con l'indicazione degli articoli giusti che andavano a confrontarsi con la situazione che si era presentata davanti al giudice interno, la Corte è riuscita ad usare lo strumento del controllo di pregiudizialità per risolvere le questioni di compatibilità tra l'ordinamento nazionale e l'ordinamento comunitario[195].

Vieppiù, la giurisprudenza in tema di tutela dei dati personali rappresenta un esempio perfetto di come la Corte di Giustizia, dopo aver più volte affermato la sua piena competenza a valutare la legittimità delle norme adottate dalle istituzioni europee rispetto ai diritti fondamentali[196] si sia spesso trovata, anche in sede di rinvio pregiudiziale, a risolvere questioni aventi ad oggetto disposizioni nazionali ritenute dal giudice remittente in contrasto con principi generali del diritto comunitario e, quindi, incompatibili con il sistema di tutela dei diritti fondamentali garantito dall'ordinamento giuridico dell'Unione[197].

Nell'ambito delle pronunce della Corte in materia di dati personali, dunque, il giudizio di proporzionalità di cui vengono onerati i giudici nazionali, oltre a non essere quasi mai privo di suggerimenti da parte della Corte di Giustizia, è comunque concepito in termini particolarmente ristretti nei confronti delle ingerenze nella vita privata previste dalle legislazioni nazionali, anche di rango costituzionale. Inoltre la Corte si spinge a riconoscere un effetto diretto in capo alle disposizioni della direttiva sulla protezione dei dati, cosicché i cittadini possono invocare direttamente dinanzi ai giudici nazionali queste previsioni paralizzando l'applicazione di norme interne contrarie alla direttiva europea[198].

Da ultimo, dall'esame delle pronunce della Corte si potrà infine notare che le problematiche inerenti alla tutela dei dati personali si caratterizzano per il fatto di lambire

[194] Cfr. punto 49 delle delle conclusioni dell'Avvocato Generale Juliane Kokott cit. sub nota 184 supra.
[195] Girolamo Strozzi, nota 142.
[196] Cfr. ex plurimis Corte di Giustizia, 28 marzo 1996, parere n. 2/94, in Racc. I-1759 punto 34
[197] Nicola Napoletano, "*La nozione di "campo di applicazione del diritto comunitario" nell'ambito delle competenze della Corte di Giustizia in tema di tutela dei diritti fondamentali*", in Diritto dell'Unione Europea, 2004, 4, p. 679 e ss.
[198] Giulia Tiberi, nota 167.

pressoché tutti i settori di competenza dell'Unione. Esistono, infatti, sentenze emesse nell'ambito di controversie in materia di concorrenza[199], di tutela della proprietà intellettuale, di aiuti di stato, di accesso ai documenti delle istituzioni e così via. Tale vastità del campo di applicazione del diritto alla tutela dei dati, suscettibile di incidere su tutti i settori di competenza dell'Unione, pare un'ulteriore conferma della sua natura di diritto fondamentale.

Fatte queste opportune premesse in linea generale, ci concentreremo ora su una selezione di casi che, ad avviso di chi scrive, appaiono significativi al punto di meritare un approfondimento. Le sentenze che prenderemo in considerazione sono quelle pronunciate dalla Corte di Giustizia nelle cause Lindqvist e Promusicae

8.1 La sentenza Lindqvist

Un caso molto interessante tra quelli trattati dalla Corte di Giustizia in materia di dati personali è quello della signora *Lindqvist*[200], avente ad oggetto la vicenda di una catechista svedese che, nell'ambito di un'attività di volontariato parrocchiale, aveva creato una pagina internet dai contenuti scherzosi inserendovi alcune informazioni personali[201] relative ai suoi colleghi, senza il loro consenso o autorizzazione. In tale pagina internet veniva riferito anche il fatto che una collega, essendosi ferita ad un piede, era in congedo parziale per malattia.

Probabilmente lo scherzo non veniva gradito da alcuni tra i soggetti interessati e, pertanto, poco tempo dopo l'apparizione della pagina web in questione, il pubblico ministero avviava un procedimento penale nei confronti della sig.ra Lindqvist per violazione della legge svedese sul trattamento dei dati personali[202].

Tra i capi di imputazione contestati alla Lindqvist figuravano quello di aver pubblicato informazioni personali di soggetti terzi senza aver acquisito il loro preventivo consenso informato e senza aver notificato il trattamento alla Datainspektion (ossia l'autorità svedese garante per il trattamento dei dati). Allo stesso modo la Lindqvist veniva accusata di aver proceduto ad un trattamento illegittimo di dati sensibili quali lo stato di salute (con particolare riferimento alla situazione della collega in congedo per malattia) e le convinzioni religiose dei suoi colleghi e, persino, di aver avviato una operazione non autorizzata di trasferimento all'estero di dati personali, per essersi avvalsa dello strumento di internet.

[199] Cfr. ex plurimis Causa C-136/79 National Panasonic Limited c. Commissione, sentenza del 26 giugno 1980 in Racc. 2057; Causa C-411/04 Salzgitter Mannesmann GmbH c. Commissione

[200] Causa C-101/01 Lindqvist, sentenza del 6 novembre 2003, in Raccolta I-12971

[201] segnatamente nomi, cognomi, numeri di telefono, situazione familiare ed informazioni sulle attività svolte durante il tempo libero

[202] Personunppgiftslag, SFS 1998, n. 204

La signora Lindqvist, che non aveva negato la ricostruzione dei fatti ma ne aveva contestato la rilevanza penale, veniva riconosciuta, in primo grado, colpevole dei reati ascritti e condannata al pagamento di un'ammenda di 4000 corone svedesi.

Successivamente, l'imputata promuoveva appello innanzi al Göta Hovrätt il quale, a sua volta, sospendeva il procedimento e rinviava alla Corte di Giustizia sottoponendo alla giurisdizione europea un'articolata serie di quesiti pregiudiziali che meritano di essere qui ricordati:

- se la creazione di una pagina internet mediante l'indicazione delle generalità, delle attività lavorative e degli interessi coltivati durante il tempo libero di una pluralità di soggetti costituiva attività di trattamento dei dati personali ai sensi della direttiva 95/46.
- Se la pubblicazione su una pagina internet privata, ma accessibile a chiunque ne conosca l'indirizzo, di informazioni personali relative a colleghi di lavoro poteva essere considerato un comportamento esulante dal campo di applicazione della direttiva [95/46] in forza di una delle eccezioni di cui all'art. 3, n. 2, della stessa.
- Se l'informazione, sempre su detta pagina, che una collega di lavoro, compiutamente individuata, si era ferita ad un piede e si trovava in congedo parziale per malattia costituiva un dato personale sensibile ai fini della predetta direttiva.
- Se una persona che si trovava in Svezia e che pubblicava dati personali su una pagina iniziale caricata su un server ivi localizzato - di modo che tali dati divenissero accessibili a cittadini di paesi terzi - trasferiva dati verso paesi terzi ai sensi della direttiva 95/46 e se la soluzione di tale questione fosse uguale anche nell'ipotesi in cui nessuna persona di un paese terzo avesse di fatto preso conoscenza dei dati ovvero nel caso in cui il server di cui si tratta si fosse trovato fisicamente in un paese terzo.
- Se le disposizioni della direttiva 95/46 ponevano limiti incompatibili con i principi generali in materia di libertà di espressione, o con altre libertà e diritti, vigenti all'interno dell'Unione europea e che trovano corrispondenza, tra l'altro, nell'art. 10 della CEDU
- Se uno Stato membro poteva, nelle circostanze indicate nelle questioni precedenti, prevedere una tutela più ampia dei dati personali o ampliare l'ambito di applicazione della direttiva [95/46], anche se non ricorreva nessuna delle condizioni di cui all'art. 13 della medesima.

Come si potrà dedurre dal nutrito elenco di quesiti che precede, sebbene la vicenda da cui era scaturito il rinvio potesse apparire banale, le questioni sollevate dal Gota Hovratt erano tutt'altro che peregrine in quanto ponevano ai massimi livelli il problema dell'interpretazione

della direttiva madre con riferimento al suo ambito di applicazione, alla nozione di trasferimento di dati personali verso paesi terzi, nonché dell'eventuale conflitto del sistema di regole da essa posto con altre libertà fondamentali.

La Corte, investita delle suddette questioni procedeva, innanzitutto, a superare numerose delle argomentazioni sollevate dalla difesa della sig.ra Lindqvist, osservando come la nozione di dati personali accolta nell'art. 3, n. 1, della direttiva 95/46 comprendesse qualsiasi informazione concernente una persona fisica identificata o identificabile, ivi compresi il nome di una persona, il suo recapito telefonico ovvero le informazioni relative alla sua situazione lavorativa o ai suoi passatempo.

Osservava, inoltre, che la pubblicazione di dette informazioni su una pagina internet costituiva, in ogni caso, un trattamento automatizzato o, comunque, parzialmente automatizzato ai sensi della precitata direttiva. Conseguenza lampante di tale osservazione era che, secondo la Corte, qualsiasi trattamento di dati personali effettuato in tal modo rientra nell'ambito di applicazione della direttiva.

Allo stesso modo, la Corte ribadiva che, laddove i dati trattati fossero idonei a rivelare una particolare condizione del soggetto interessato con riferimento al suo stato di salute, alle sue convinzioni religiose, politiche o filosofiche, come pure ai propri orientamenti sessuali, il dato personale rientrava nella categoria speciale dei dati sensibili soggetti, ai sensi della direttiva comunitaria e delle normative nazionali, a regole più stringenti.

Fin qui nulla di nuovo, dunque, alla luce del precedente panorama normativo o giurisprudenziale.

Assolutamente inedita è, invece, la posizione della Corte in merito all'esclusione della possibilità di considerare il trattamento di dati personali su internet in termini di trasferimento all'estero ai sensi dell'art. 25 della direttiva 95/46/CE.

Infatti, secondo le osservazioni presentate alla Corte dalla Commissione e dal Governo svedese si doveva ritenere che l'inserimento, tramite computer, di dati personali su una pagina Internet maniera tale da renderli accessibili a cittadini di paesi terzi, costituiva un trasferimento di dati verso paesi terzi ai sensi della direttiva 95/46. La risposta, nell'ottica della Commissione, sarebbe stata la stessa se nessun cittadino di un paese terzo avesse preso effettivamente conoscenza dei suddetti dati o se il server in cui essi erano caricati si fosse trovato, fisicamente, nel paese terzo.

La posizione della Commissione, quale condivisa dal governo svedese muoveva,dunque, dall'esigenza di corredare l'art. 25 della direttiva di un'interpretazione il più possibile ampia. La Commissione, infatti, era preoccupata che una lettura restrittiva dell'art. 25 della direttiva

applicata al mondo di internet potesse comportare un abbassamento del livello di protezione garantito nel territorio dell'Unione, determinando un potenziale trasferimento di dati personali verso paesi terzi, ivi inclusi quelli in cui non è garantito alcun livello di protezione dei dati ovvero, ove tale protezione risulti essere inadeguata rispetto a quella esistente nella UE[203].

La Corte di Giustizia, invece, dopo aver rilevato l'assenza di una nozione precisa di "trasferimento all'estero di dati personali" all'interno della direttiva, osservava che le informazioni che si trovavano su Internet potevano essere consultate da un numero indefinito di persone residenti in molteplici luoghi, in qualsiasi momento. In particolare, per ottenere le informazioni che figuravano sulla pagina Internet caricata dalla sig.ra Lindqvist, l'utente di Internet doveva non soltanto collegarsi a quest'ultima, ma anche effettuare le azioni necessarie per scaricarne il contenuto e consultarla. In altri termini, la pagina Internet della sig.ra Lindqvist non conteneva alcun meccanismo suscettibile di comportare un invio automatico di tali informazioni a persone che non avessero deliberatamente cercato di accedere a dette pagine. Pertanto, sempre secondo la Corte, la mera immissione dei dati in rete non poteva comportare di per sé un "trasferimento" ai sensi dell'art. 25 della direttiva 95/46.

Ad avviso di chi scrive la posizione della Corte appare ragionevole in quanto, ove si volesse accogliere l'estensione dell'art. 25 al mondo di internet, gli Stati dell'UE sarebbero chiamati ad intervenire continuamente per valutare il livello di protezione assicurata ai dati personali nel Paese in cui si trovi ubicato di volta in volta l'occasionale *surfer* che scarichi dati pubblicati in rete, col rischio di paralizzare proprio la libertà di circolazione delle informazioni all'interno ed all'esterno dell'Unione, che è proprio l'obiettivo stesso che la stessa direttiva si prefigge.

Come si è già visto, inoltre, una delle questioni pregiudiziali sottoposte all'esame della Corte nel caso Lindqvist verteva sul quesito se il pubblicare su una pagina iniziale privata, ma accessibile a chiunque ne conosca l'indirizzo, dati relativi a colleghi di lavoro poteva essere considerato come un comportamento non rientrante nell'ambito di applicazione della direttiva [95/46] in forza di una delle eccezioni di cui all'art. 3, n. 2, della stessa.

Notoriamente, secondo quest'ultima disposizione, la direttiva non trova applicazione nei confronti dei trattamenti di dati effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica

[203] Rocco Panetta, "*Trasferimento all'estero di dati personali e internet: storia breve di una difficile coabitazione*", in *Diritto dell'Unione Europea*, 2004, 4, pag. 1014

sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale, nonché nei confronti dei trattamenti di dati effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

L'avvocato generale Tizzano aveva concluso per la non applicabilità della direttiva 95/46 al caso Lindqvist in quanto trattavasi di attività esulante dal campo di applicazione del diritto comunitario[204]. In particolare, secondo l'Avvocato Generale la pagina internet in questione era stata creata dalla signora Lindqvist, senza alcun intento di sfruttamento economico, esclusivamente come supporto per l'attività di catechesi svolta, a titolo gratuito e al di fuori di qualsiasi rapporto lavorativo, in seno alla comunità parrocchiale. Il trattamento di dati personali era stato dunque effettuato per un'attività che non presentava nessun legame (o quanto meno nessun legame diretto) con l'esercizio delle libertà fondamentali garantite dal Trattato e non formava oggetto di alcuna specifica disciplina a livello comunitario"[205].

In buona sostanza le conclusioni dell'Avvocato Generale si basavano su un assunto chiaro e, per certi versi, condivisibile: non si può considerare come norma di trasposizione qualsiasi disposizione nazionale che intervenga nella materia oggetto di una direttiva di armonizzazione "*facendo poi discendere da tale premessa che ogni trattamento previsto da una disposizione nazionale è coperto dalle disposizioni della direttiva in quanto per definizione effettuato per lo svolgimento di un'attività compresa nel campo di applicazione del diritto comunitario"*.

La direttiva di armonizzazione, sempre secondo l'Avvocato Generale, anche qualora preveda di stabilire un livello di tutela "equivalente in tutti gli stati membri" al fine di eliminare le eventuali disparità e nonostante miri nel contempo a garantire un "elevato grado" di salvaguardia dei diritti fondamentali della persona, ha comunque come scopo quello di dettare principi comuni volti al ravvicinamento di quelle disposizioni nazionali che abbiano per oggetto l'instaurazione ed il funzionamento del mercato interno (art. 95 CE). In quest'ottica la salvaguardia dei diritti fondamentali non rappresenta un "*autonomo obiettivo dell'atto comunitario*" a meno che non si voglia giungere alla incongrua conseguenza di far rientrare nel suo campo di applicazione anche trattamenti effettuati per l'esercizio di attività

[204] Cfr. punto 44 delle conclusioni dell'Avvocato Generale Antonio Tizzano nell'ambito della causa Causa C-101/01 "*Alla luce dell'insieme delle considerazioni che precedono, propongo dunque di rispondere al presente quesito che, ai sensi dell'art. 3, n. 2, primo trattino, della direttiva, non rientra nel campo di applicazione della direttiva stessa un trattamento di dati personali consistente nella creazione, senza alcun intento di sfruttamento economico, di una home page del tipo di quella in esame, che sia destinata esclusivamente a supportare l'attività di catechesi svolta, a titolo gratuito e al di fuori di qualsiasi rapporto lavorativo, in seno alla comunità parrocchiale".*

[205] Cfr. punto 36 delle conclusioni dell'Avvocato Generale Antonio Tizzano nell'ambito della causa Causa C-101/01 Lindqvist

che non presentino alcun rapporto con l'instaurazione ed il funzionamento del mercato interno.

La Corte di Giustizia disattendendo le Conclusioni dell'Avvocato Generale nella causa *Lindqvist* si è pronunciata per l'applicabilità della direttiva di armonizzazione nei casi di specie, affermando come il margine di discrezionalità offerto agli stati dalla direttiva non produce di per sé l'effetto di sottrarre l'atto al controllo giurisdizionale della Corte. Se così fosse, infatti, si produrrebbe nel sistema una lacuna nel controllo giurisdizionale su tutti quegli atti che, per loro stessa natura, hanno l'obiettivo di armonizzare le legislazioni nazionali attraverso un'obbligazione di risultato, lasciando invece alla libera discrezionalità degli Stati membri l'attuazione del contenuto dell'atto in questione. Del resto nella sentenza *Lindqvist* la Corte afferma che la direttiva che attribuisce agli stati membri un ambito di discrezionalità è comunque suscettibile di controllo giurisdizionale in punto di validità[206]. In questi termini quanto sostenuto dalla Corte non può significar altro che un ampliamento implicito delle competenze delle istituzioni europee anche in materia di diritti fondamentali giustificato e legittimato dalla Corte stessa attraverso l'esercizio "*in qualità di arbitro ultimo dei conflitti sull'estensione delle competenze*" della sua "kompetenz-kompetenz giurisdizionale"

In conclusione la sentenza Lindqvist è molti significativa perché con essa la Corte afferma il principio per cui nel caso in cui una direttiva attribuisca agli Stati membri il potere di adottare deroghe suscettibili di incidere su un diritto fondamentale dell'individuo è anche la legittimità delle sue stesse disposizioni a poter essere valutata alla luce delle norme che tutelano tale diritto fondamentale. In altri termini i diritti fondamentali diventano il parametro che la Corte utilizza sia per sindacare la legittimità tanto degli atti comunitari quanto degli atti normativi interni che a questi danno attuazione[207]. Tale sindacato sulla normativa interna di trasposizione non costituisce, peraltro una novità. Come è stato giustamente osservato in dottrina[208], infatti, a seguito delle modifiche apportate dal Trattato di Amsterdam in materia di rispetto dei diritti dell'uomo e delle libertà fondamentali quali "principi generali del diritto comunitario" è derivato un limite all'esercizio delle competenze non soltanto per le istituzioni europee, ma anche a carico degli stessi Stati membri (eccezion fatta ovviamente per le materie

[206] Alice Pisapia, "*Una sentenza additiva in punto di attuazione della direttiva sul ricongiungimento familiare",* in Giustizia Civile, 2007, 3, pag. 544

[207] Fabio Macrì, "*La Corte di Giustizia sul diritto al ricongiungimento familiare: la sentenza Parlamento c. Consiglio*", in Diritto dell'Unione Europea, 2006,4, pag. 203

[208] cfr. V.S. Negri, "La tutela dei diritti fondamentali nell'ordinamento comunitario alla luce del Trattato di Amsterdam", 1997 p. 788 e ss.

di loro esclusiva competenza) in quanto principi "comuni alle loro tradizioni costituzionali[209]."

Pertanto, la sentenza Lindqvist conferma l'attribuzione alla Corte del potere di bilanciare diritti nascenti da fonti comunitarie e diritti fondamentali, che dovrebbero trovare la loro autentica radice nelle costituzioni nazionali[210]. Nella sentenza Lindqvist, infatti, l'equilibrio tra libertà di espressione e le limitazioni stabilite dalla direttiva sui dati personali è dalla Corte individuato nella stessa direttiva 95/46 , ma in secondo luogo nel dovere delle autorità e dei giudici degli Stati membri non solo di interpretare il diritto nazionale in modo conforme alla direttiva comunitaria ma anche di provvedere a non fondarsi su un'interpretazione di quest'ultima che entri in conflitto con i diritti fondamentali tutelati dall'ordinamento giuridico comunitario o con gli altri principi generali del diritto comunitario come ad esempio il principio di proporzionalità[211] .

8.2 La sentenza Promusicae

Un altro caso interessante in materia di tutela dei dati personali deciso dalla Grande Sezione della Corte di Giustizia è il caso Promusicae[212], avente ad oggetto una controversia tra la l'associazione senza scopo di lucro Productores de Música de España (Promusicae) (in prosieguo: la «Promusicae») e la Telefónica de España SAU (in prosieguo: la «Telefónica») in merito al rifiuto, da parte di quest'ultima, di comunicare alla Promusicae, che agiva per conto dei titolari di diritti di proprietà intellettuale che ne fanno parte, una serie di dati personali relativi all'utilizzo di Internet mediante connessioni fornite dalla Telefónica. La questione all'esame della Corte non era affatto peregrina giacché verteva sul problema del corretto bilanciamento tra diritti fondamentali di pari rango, segnatamente tra l'esigenza di proteggere i diritti di proprietà intellettuale e il diritto d'autore e la tutela dei dei dati personali.

In particolare la Promusicae aveva presentato, innanzi al Tribunale commerciale di Madrid, una domanda avente ad oggetto un ordine di esibizione nei confronti della

[209] cfr. Nicola Napolitano, nota 197
[210] cfr. Nicola Napoletano, nota 197
[211] Federico Sorrentino "LA tutela multilivelli dei diritti", in Rivista Italiana di Diritto Pubblico Comunitario, 2005, 1 , pag. 91 e ss.
[212] Causa C-275/06 Productores de Musica Espana c. Teléfonica de Espana, sentenza del 29 gennaio 2008, in Raccolta I-278

Telefonica. Per la precisione, la Promusicae chiedeva che il Tribunale ordinasse alla Telefónica di rivelare l'identità e l'indirizzo fisico di talune persone alle forniva il servizio di accesso ad Internet (che la Promusicae aveva identificato mediante l'indirizzo IP[213] e la data e l'ora di connessione), rilevando, altresì, come queste persone, utilizzando il programma di scambio di archivi (cosiddetto «peer to peer[214]» ovvero «P2P») denominato «KaZaA», commettessero atti di concorrenza sleale e violazione dei diritti di proprietà intellettuale mediante il download di materiale coperto da copyright. In altri termini, la comunicazione dei dati personali di queste persone, era funzionale alle cause civili che la Promusicae intendeva avviare nei confronti delle stesse.

Il Tribunale Commerciale di Madrid accoglieva la domanda ed emetteva ordinanza con la quale ingiungeva alla Telefonica di comunicare i dati richiesti. Tuttavia la Telefonica presentava opposizione avvero la predetta ordinanza sostenendo come, in base al diritto spagnolo[215], la trasmissione dei dati richiesti poteva essere autorizzata esclusivamente nell'ambito di un'indagine penale o per la tutela della pubblica sicurezza e della difesa nazionale e non anche nel contesto di un procedimento civile.

Il Tribunale Commerciale sospendeva, quindi, il giudizio e rinviava alla Corte di Giustizia. Il quesito oggetto del rinvio pregiudiziale era sostanzialmente il seguente: se il diritto comunitario, e in particolare le direttive 2000/31, 2001/29 e 2004/48, lette anche alla luce degli artt. 17 e 47 della Carta, andavano interpretate nel senso che impongono agli Stati membri di istituire, al fine di garantire l'effettiva tutela del diritto d'autore, l'obbligo di comunicare taluni dati personali nel contesto di un procedimento civile.

La Corte osservava, anzitutto, come la questione sottopostale, oltre a concernere la tutela della proprietà individuale, fosse rilevante anche sotto il profilo della protezione dei diritti fondamentali, in particolare della tutela dei dati personali disciplinata. Ciò premesso, la Corte affermava che gli Stati membri sono tenuti, in occasione della trasposizione delle direttive comunitarie, a fondarsi su un'interpretazione di queste ultime tale da garantire un giusto equilibrio tra i diversi diritti fondamentali tutelati dall'ordinamento giuridico comunitario.

[213] L'indirizzo IP è una sequenza numerica, simile ad un numero di telefono, necessaria per far comunicare in Internet i dispositivi in rete. Ogniqualvolta si accede ad una pagina internet, al computer sul quale è salvata la pagina viene comunicato l'indirizzo IP del computer che la consulta, così che i dati possono essere trasmessi da un computer all'altro tramite Internet. L'indirizzo IP fornito dall'ISP (Internet Service Provider, es. "Virgilio" o "Alice") può essere fisso o, come il più delle volte accade, "dinamico" ed essere cioé assegnato di volta in volta dall'ISP ad ogni connessione.

[214] Trattasi di un'operazione di cd. "*filesharing"* che è una forma di scambio di file, ad esempio brani musicali o film. Gli utenti copiano dapprima i file sui loro computer e li offrono successivamente in condivisione a chiunque sia loro connesso via Internet tramite un particolare programma, quale ad es. "Kazaa".

[215] In particolare in base alla Ley 34/2002 de servicios de la sociedad de la información y de comercio electrónico; BOE 12 luglio 2002, n. 166, pag. 25388

Inoltre, in sede di attuazione delle misure di recepimento di tali direttive, le autorità e i giudici degli Stati membri devono non solo interpretare il loro diritto nazionale in modo conforme alle dette direttive, ma anche provvedere a non fondarsi su un'interpretazione di esse che entri in conflitto con i summenzionati diritti fondamentali o con gli altri principi generali del diritto comunitario, come, ad esempio, il principio di proporzionalità

Ciò premesso, la Corte di Giustizia dava soluzione al quesito formulato dal giudice di rinvio affermando che il diritto comunitario, in linea di principio, consente pur senza tuttavia imporre agli Stati membri la trasmissione dei dati personali sul traffico delle comunicazioni concernenti l'utilizzo di Internet ai titolari dei diritti di proprietà intellettuale anche nell'ambito di un procedimento civile.

In tal senso la Corte si è pronunciata in senso profondamente difforme rispetto a quanto ritenuto dall'avvocato generale Kokott nelle sue conclusioni[216], secondo le quali "*le disposizioni comunitarie in materia di protezione dei dati relativi alle comunicazioni elettroniche consentono di trasmettere i dati sul traffico delle comunicazioni personali esclusivamente alle autorità statali competenti, e non direttamente ai titolari di diritti d'autore, che vogliano far valere in sede civile la violazione dei loro diritti*[217]" . In altri termini, come giustamente osservato dall'avvocato generale, la comunicazione dei dati degli utenti internet può essere ammesse soltanto nell'ambito di un procedimento penale e non anche nel quadro di una causa civile, ove implicherebbe una deroga eccessivamente estesa e, per altri, versi indeterminata al principio della tutela dei dati personali. Invero, per riprendere quanto magistralmente argomentato dall'avvocato generale Kokott "u*n'interpretazione dell'art. 6, n. 6, della direttiva 2002/58/CE che consenta la comunicazione dei dati sul traffico alla potenziale controparte semplicemente in forza di un loro uso in un procedimento contenzioso sarebbe ... incompatibile con il principio di prevedibilità che deve essere osservato quando si giustificano per legge ingerenze nella sfera della vita privata e nella tutela dei dati",* dal momento in cui *"l'utente dovrebbe sempre aspettarsi, e non solamente in seguito ad una violazione dei diritti d'autore, che i suoi dati sul traffico siano trasmessi a terzi che, per un qualsivoglia motivo, vogliono intentargli causa. È da escludere che siffatte controversie si fondino in tutti i casi su un'esigenza sociale imperativa ai sensi della giurisprudenza concernente l'art. 8 CEDU*"[218].

[216] Causa C-275/06, conclusioni dell'avvocato generale Juliane Kokott presentate il 18 luglio 2007
[217] V. Punto 3 delle conclusioni dell'avvocato generale Juliane Kokott cit. sub nota 211 supra.
[218] V. Punto 43 e ss. delle conclusioni dell'avvocato generale Juliane Kokott cit. sub nota 211 supra.

In definitiva, nonostante parte della dottrina ritenga che la Corte, nell'ambito della causa Promusicae, abbia adottato una soluzione di neutralità "elvetica"[219] , a parere di chi scrive non vi è ombra di dubbio che la sentenza in esame venga piuttosto incontro alle posizioni delle case musicali, preoccupate dalla timidezza con la quale le giurisdizioni nazionali tendono a perseguire in sede penale il fenomeno del cd. "Peerto peer" [220]. In quest'ottica, che l'atteggiamento soltanto apparentemente pilatesco della Corte di Giustizia abbia comportato, in astratto, una vittoria della proprietà intellettuale sulla tutela dei dati personali non pare possa essere messo in dubbio. Infatti, questa sentenza, che lascia alla discrezionalità degli Stati membri la possibilità di estendere l'obbligo di comunicazione dei dati personali degli utenti di internet anche ai procedimenti civili rappresenta un vero e proprio cavallo di Troia attraverso il quale il bilanciamento tra tutela della proprietà intellettuale e tutela dei dati personali rischierà di essere irrimediabilmente compromesso a verosimile detrimento di quest'ultimo, specie in quegli Stati in cui il processo legislativo è noto per risentire fortemente dell'influenza dei gruppi di pressione. Lo scenario che potrebbe aprirsi, infatti, è quello di Stati che prevedono la possibilità di comunicazione dei dati personali anche nell'ambito di procedimenti civili e Stati che non prevedono questa possibilità, con buona pace per le esigenze di armonizzazione ed uniforme applicazione del diritto dell'Unione Europa anche nella prospettiva di un elevato standard di protezione dei diritti fondamentali. Non a caso la sentenza Promusicae è stata salutata con favore proprio dai sostenitori del diritto d'autore[221], per i quali, nell'ambito del conflitto tra diritto alla privacy e diritto d'autore, debba prevalere quest'ultimo[222].

Vale pena, dunque, di augurarsi che gli Stati membri che vorranno (o verranno indotti a) cogliere l'opportunità offerta da questa sentenza facciano tesoro dell'invito contenuto nella Sentenza Promusicae secondo cui la limitazione della protezione dei dati personali dovrà avvenire unicamente in funzione di ciò che è strettamente necessario per assicurare la difesa effettiva del diritto d'autore[223]. In altri termini, l'invito che i giudici di Lussemburgo

[219] L'espressione è di Cristophe Caron, "*Appréciation de l'obbligation de communiquer des données à caractère personnel dans le cadre d'une procedure civile* », in « *La Semaine Juridique Entreprise et Affaires* » n° 9, 28 Février 2008, 1270

[220] Alessandro Mantelero "*L'idra del peer to peer, tra tutela della privacy ed enforcement del diritto d'autore*," in Rivista Trimestrale di Diritto e Procedura Civile 2008, 4, 1482 e ss

[221] Gaia Mari, L'unione Europea impone di non sacrificare ad occhi chiusi la proprietà intellettuale sull'altare della privacy" in Diritto D'Autore, 2008,2, 289 e ss

[222] Pierluigi Di Maio, "Il rapporto tra diritto d'autore e diritto alla riservatezza. Recenti sviluppi nella giurisprudenza comunitaria", in Il Diritto D'Autore, 2010, 1, p. 20

[223] Elsa Bernard, "Droits d'auteur et protection des droits fondamentaux", in Revue Europe n° 3, Mars 2008, comm. 98

rivolgono agli Stati tra le righe della sentenza in esame è a non sacrificare la tutela dei dati personali sull'altare della lotta alla contraffazione ed alla pirateria audiovisiva.

In ogni caso nella successiva sentenza Scarlett[224], avente ad oggetto una vicenda analoga, la Corte sembra aver ripreso in mano le redini della tutela dei diritti fondamentali della persona. Nel quadro della lotta alla pirateria audiovisiva, la SABAM, società belga degli autori ed editori, aveva intentato un'azione civile contro un Internet Service Provider di nome "Scarlet", lamentando come lo stesso permettesse ai suoi utilizzatori degli scambi di files attraverso il noto sistema del peer to peer, in violazione del diritto d'autore. La SABAM chiedeva, dunque, al giudice belga di ordinare alla Scarlet la predisposizione di un sistema di filtraggio preventivo tale da permettere di identificare le violazioni al diritto d'autore e di bloccare gli scambi. Investita del rinvio pregiudiziale da parte del giudice interno, la Corte ha concluso in senso conforme all'Avvocato Generale Cruz Villalòn[225] per l'incompatibilità con il diritto europeo di un'ingiunzione, come quella richiesta dalla SABAM, che si applichi in via preventiva, senza cioè che sia stata concretamente accertata una violazione, indistintamente a tutta la clientela, senza limitazione di tempo e a spese esclusive della Scarlet[226].

[224] Causa C-70/01, Scarlet Extended SA, sentenza del 24 novembre 2011

[225] Anna Saraceno "Note in tema di violazione del diritto d'autore tramite internet: la responsabilità degli Internet Service Providers", in Rivista di Diritto Industriale, 2011, 6, pg. 375

[226] Laurence Idot, "Internet, piratage et obligations de filtrer les comunications éléctroniques » in Revue Europe n° 1, Janvier 2012, comm. 44

CAPITOLO III

LA PROPOSTA DI RIFORMA DEL QUADRO LEGISLATIVO EUROPEO DI PROTEZIONE DEI DATI PERSONALI

1. Conderazioni generali

In data 25 gennaio 2012 la Commissione Europea, in attuazione del mandato ricevuto nel quadro del Programma di Stoccolma, ha annunciato la pubblicazione di una proposta di integrale riforma della legislazione europea in materia di protezione dei dati personali.

L'iniziativa, che si inserisce nell'ambito del programma denominato "*Agenda Digitale per l'Europa*[227]" e, più in generale, nell'ambito della "*Strategia Europa 2020*[228]", è orientata al perseguimento di due obiettivi essenziali: da un lato quello di rafforzare il diritto alla protezione dei dati personali quale diritto fondamentale, così come affermato dalla Carta dei Diritti Fondamentali (art. 8) e dal Trattato di Lisbona (art. 16 TFUE). Dall'altro, quello di promuovere il consolidamento del mercato digitale europeo, favorendo la creazione di nuove opportunità commerciali e lavorative nel settore della *digital economy*, nonché accrescendo la fiducia dei cittadini verso i servizi online[229].

Il progetto di riforma varato dalla Commissione si pone, altresì, in sinergia con le analoghe iniziative da parte di altre organizzazioni internazionali. Oltre all'Unione Europea, infatti, anche il Consiglio d'Europa sta valutando in che modo la Convenzione per la protezione degli individui con riguardo al trattamento automatizzato di dati (la cd. "Convenzione 108") possa essere modificata al fine di rispondere meglio alle sfide del presente[230] e lo stesso dibattito sta interessando, altresì, le Linee Guida varate nell'ambito dell'Organizzazione per la Cooperazione e lo Sviluppo in Europa[231] (cd. "*OECD guidelines*").

[227]Cfr. Comunicazione della Commissione Europea in merito all'Agenda Digitale per l'Europa reperibile sul sito http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT

[228] Cfr. sito web della Strategia Europa 2020 http://ec.europa.eu/europe2020/index_en.htm

[229] Cfr. Commissione Europea "*Why do we need a data protection reform*", factsheet consultabile su http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/1_en.pdf

[230]Vedi proposta per la modernizzazione della convenzione 108, reperibile su http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf

[231] Cfr. il rapporto OCSE *Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines*, 6 aprile 2011 reperibile su http://www.oecd.org/dataoecd/22/25/47683378.pdf e la Dichiarazione di Seoul sul Futuro della Internet Economy del giugno 2008 reperibile su http://www.oecd.org/dataoecd/49/28/40839436.pdf

Numerose sono, infatti, le ragioni che, a distanza di ben 17 anni dall'adozione della Direttiva 95/46/CE sulla protezione dei dati personali e sulla libera circolazione di tali dati, spingono per l'opportunità di una riforma integrale dell'edificio normativo europeo.

Innanzitutto, il recente ed esponenziale sviluppo tecnologico legato all'informatica e ad internet unitamente alla globalizzazione dei costumi e della società, ha cambiato radicalmente le modalità attraverso le quali oggi i dati personali vengono raccolti e gestiti, richiedendo una ri-attualizzazione della disciplina vigente.

Come opportunamente osservato dal Commissario alla Giustizia Viviane Reding in occasione della presentazione del progetto di riforma, infatti, all'epoca dell'entrata in vigore della Direttiva 95/46/CE sulla protezione dei dati personali, meno dell'un per cento dei cittadini europei faceva uso di internet[232]. Oggi, al contrario, la pressoché totalità dei cittadini europei dispone di un accesso alla rete, ove possono essere scambiate e trasferite enormi quantità di dati in semplici frazioni di secondo. Anche l'avvento dei social networks, se da un lato ha rivoluzionato il modo in cui oggi si mantengono i contatti informali con amici e colleghi di lavoro, rendendo pressoché obsoleta la corrispondenza epistolare, dall'altro ha esposto la privacy degli utenti a nuove e pericolose forme di controllo e di ingerenza, suscettibili di avere ripercussioni potenzialmente negative sul piano lavorativo, sociale e familiare[233].

In secondo luogo, occorre sottolineare come, da diverso tempo oramai, il livello di armonizzazione ottenuto con la trasposizione della Direttiva 95/46/CE non risulti più accettabile, essendo registrabili delle divergenze talvolta vistose in seno alle legislazioni di ciascuno Stato membro. Invero, nonostante la Direttiva del 1995 abbia avuto il merito di riavvicinare le legislazioni nazionali esistenti (ovvero di obbligare gli Stati a dotarsi di una legislazione *ad hoc*) e di costituire, per oltre diciassette anni, il parametro di riferimento in materia di protezione dei dati personali, è pur vero che lo strumento é stato recepito in maniera comunque difforme all'interno dei vari ordinamenti nazionali[234].

Tale fattore ha comportato e tutt'oggi comporta incertezze a livello giuridico, inefficienza economica e maggiori oneri ed adempimenti per le amministrazioni e l'industria. Le diversità registrabili nella normativa degli Stati membri, infatti, alterano il funzionamento del mercato

[232]Comunicato stampa del Commissario Giustizia Viviane Reding consultabile su http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=en&guiLanguage=en aggiornato al 1 settembre 2012

[233] Cfr. Commissione Europea "*How will the EU data protection reform affect social networks*", reperibile su http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf

[234] Ariane Siege, William Denny "*Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*", in The Business Lawyer 65 no1 285-307 N 2009

interno e la cooperazione tra le autorità pubbliche con riferimento alle politiche europee, creando confusione e dubbi e provocando una perdita di fiducia da parte dei cittadini[235]. Inoltre, la forte riaffermazione della protezione dei dati personali quale diritto fondamentale della persona, sia da parte dell'art. 8 della Carta Europea dei Diritti Fondamentali che dell'art. 16 del TFUE, esige che venga garantita una efficace ed uniforme protezione dei cittadini europei su tutto il territorio europeo.

A tutto questo si deve aggiungere che la mancanza di uniformità in questo campo indebolisce la capacità dell'Unione Europea di parlare con una sola voce a livello internazionale[236], specie con riferimento ai negoziati con gli Stati terzi volti alla conclusione di accordi sul trasferimento dei dati.

Come si può comprendere, dunque, la volontà di rafforzare i diritti dei singoli, l'esigenza di tutelare il funzionamento del mercato interno, nonché quella di assicurare un elevato livello di tutela anche con riguardo ai trasferimenti di dati all'estero hanno fatto si che l'Unione Europea oggi non sia più disposta a tollerare l'esistenza di diversi quadri legislativi nazionali sulla protezione dei dati, sia con riferimento al loro contenuto che alla loro efficacia[237].

Su di un versante parallelo, poi, un ulteriore aspetto che ha reso necessaria la riforma dell'attuale sistema normativo è dovuto alla necessità di garantire una maggiore sicurezza dei dati raccolti, specialmente online. Anche qui, lo sviluppo tecnologico dell'informatica non ha soltanto apportato benefici, ma ha altresì creato le condizioni per l'insorgere di nuove minacce per la privacy individuale. La presenza di programmi insidiosi quali *trojans*, *cookies*, *malware* e *virus* rappresenta un rischio concreto per la privacy degli utenti durante la navigazione su internet, mettendo a rischio la sicurezza dei dati personali e di altre informazioni importanti quali quelle concernenti i dettagli delle carte di credito, la sicurezza dei sistemi di pagamento online e le coordinate bancarie.

Meno frequenti ma non per questo meno pericolosi si sono rivelati poi i cd. "*data security breach*", ossia quegli accessi non autorizzati da parte di pirati informatici ai database di grosse aziende o di amministrazioni pubbliche contenenti le informazioni personali di migliaia (se non milioni) di persone. Si tratta di veri e propri attacchi che spesso non perseguono un intento meramente dimostrativo. Nell'aprile del 2011 la società giapponese Sony, ad esempio, ha subito un attacco di questo genere che ha comportato il trafugamento, da parte di ignoti,

[235] Cfr. Commissione Europea "*How will the EU data protection reform strengthen internal market*" , reperibile su http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf
[236] Luis Costa, Yves Poullet in "Privacy and the regulation of 2012", Computer Law & Security Review, June 2012, Vol. 28 Issue 3,p 9 p . 254262
[237] Idem

delle informazioni personali e delle informazioni relative alle carte di credito di 77 milioni di utenti del circuito "Playstation", la popolare consolle per video giochi[238].

Orbene, non costituisce certo un mistero il fatto che le informazioni personali così carpite possono essere utilizzate nei modi più disparati, dall'invio massiccio di e-mail spazzatura (cd. spamming), ai furti di identità e alle frodi online[239].

Ciò premesso, il progetto di riforma varato dalla Commissione ha conosciuto un intenso periodo di gestazione durato almeno un paio d'anni. Detta gestazione, che ha preso inizio mediante la presentazione della Comunicazione denominata "*A comprehensive approach on personal data protection in the European Union*", pubblicata in data 4 novembre 2010[240], ha dato luce a due testi normativi che compongono, unitamente alla comunicazione denominata "*Safeguarding Privacy in a connected world: A european data protection frame work for the 21st centrury*"[241] l'attuale pacchetto di riforma: da un lato una proposta di Regolamento[242] tesa a sostituire la Direttiva 95/46 e a modificare la Direttiva 2002/58/CE, dall'altro, la proposta di una Direttiva[243] riguardante il trattamento di dati personali da parte delle competenti autorità per finalità di prevenzione, indagine, accertamento o perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, diretta a sostituire la Decisione Quadro 2008/977/JHA.

La dottrina ha accolto con particolare interesse l'annuncio del progetto di riforma. In particolare, è stato osservato che, mentre la sostituzione della Decisione Quadro sulla protezione dei dati nei procedimenti penali di polizia presenta un valore più semantico che sostanziale, non apportando cambiamenti significativi ai principi vigenti, l'abrogazione della Direttiva 95/46 sulla protezione dei dati costituisce, al contrario, uno sviluppo importantissimo che, una volta finalizzato, influenzerà la vita e il lavoro degli europei[244].

Allo stesso modo, parte della dottrina ha criticato la scelta della Commissione di optare per l'emanazione di due distinti testi legislativi. E' stato osservato come questo approccio non

[238] Clark Boyd, "Global impact of Sony security breach" reperibile su http://www.theworld.org/2011/04/sony-security-breach/ aggiornato al 1 settembre 2012

[239] E' stato osservato che simili attacchi informatici possono essere impiegati anche da parte di regimi autoritari per fini di repressione dell'opposizione politica, delle libertà di stampa e di espressione.

[240] Testo reperibile su http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf

[241] Testo reperibile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0009:FIN:EN:PDF

[242] Il testo della proposta di regolamento è reperibile sul sito della Commissione http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[243] Testo reperibile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52012PC0010:en:NOT

[244] Françoise Gilbert, "*EU Data Protection Overhaul, New Draft Regulation*" in The Computer & Internet Lawyer Vol 29 No 3 March 2012

sia in grado di apportare alcun beneficio con riguardo ai dichiarati obiettivi di protezione[245]. Infatti, la Commissione aveva due possibilità: o scegliere di sostituire Direttiva e Decisione quadro per mezzo di un unico strumento normativo in materia di protezione dei dati, ovvero emendare ciascuno di essi nel panorama post-Lisbona. La scelta di seguire questa seconda soluzione, sebbene realistica, si risolve nell'introduzione di una ingiustificata distinzione tra il regime di tutela generale dei dati personali e quello relativo alla tutela dei dati con riguardo alla cooperazione di polizia e giudiziaria in materia penale. Secondo il citato orientamento detta distinzione, che viene mantenuta nella riforma, si è dimostrata negli anni essere eccessivamente schematica ed artificiosa[246]. Oggi, infatti, i database di informazioni personali creati da parte dei privati per finalità di trattamento possono essere ceduti ad agenzie governative. Mantenere due distinti regimi di protezione dei dati personali risulta essere, nella pratica, estremamente difficile, se nono impossibile, sicché la Commissione rischia di prolungare l'ambiguità in questo campo ogniqualvolta il settore privato e gli organi di polizia interagiscono[247].

Anche per il Garante Europeo per la Protezione dei dati la scelta operata dalla Commissione non rappresenta affatto un passo in avanti verso un sistema omogeneo di protezione dei dati[248]. Secondo il Garante, infatti, la Commissione avrebbe potuto fare uso di un unico regolamento per entrambe le discipline salvo riservarsi la possibilità di integrare, in seguito, le disposizioni di carattere generale con un set addizionale di regole settoriali.

In altre parole il Garante segnala il rischio che i due strumenti normativi subiscano un'evoluzione difforme o comunque tale da distanziare notevolmente il rispettivo livello di protezione, generando discrasie e problemi di coordinamento. Invero, la scelta di uno strumento autonomo per quanto riguarda la tutela dei dati personali nel campo della cooperazione penale appare, aglio occhi del Garante, disdicevole proprio alla luce della crescente interazione tra il settore privato e le autorità di pubblica sicurezza[249]. Un lampante esempio di tale interazione è costituito dal trasferimento dei dati PNR da parte delle compagnie aeree alle autorità di pubblica sicurezza degli USA. Senza contare poi che oggi, sempre secondo il parere del Garante Europeo, non si può neppure escludere un processo inverso e che, comunque, il mantenimento di tale regime diversificato risulta ancora più

[245] Paul De Hert, Vagelis Papakonstantinou, "*The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*" in Computer Law & Security Review 28 (2012) 130- 142
[246] Idem
[247] Ibidem19
[248] Cfr. punto 19 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012, reperibile al sito http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf aggiornato al 1 settembre 2012
[249] Cfr. punto 38 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012

complesso in relazione a quei sistemi informativi istituiti in parte nel settore della cooperazione penale e in parte in altri settori. Basti pensare al Sistema di Informazione Schengen [250].

Ciò premesso, la proposta di Regolamento è stata inoltrata al Parlamento Europeo ed al Consiglio al fine di essere adottata mediante la procedura di co-decisione, ossia la procedura legislativa ordinaria. Essa entrerà formalmente in vigore decorsi due anni dalla sua adozione formale. Sicché si può ragionevolmente preventivare che, per la fine del 2014, il nuovo Regolamento sarà una realtà normativa a tutti gli effetti.

E' evidente, dunque, che il testo attualmente licenziato dalla Commissione subirà, con ogni probabilità, delle modifiche, soprattutto in funzione delle osservazioni che verranno fatte dall'Europarlamento, particolarmente attento alle questioni inerenti i diritti fondamentali come testimoniato dalle "battaglie" condotte in occasione della conclusione del trattato PNR, del Trattato" Swift" e, più recentemente, dal Trattato "ACTA".

Un così lungo ed intenso iter legislativo non pare comunque ingiustificato. Gli obiettivi della riforma sono particolarmente elevati, in quanto essa andrà a sostituire una disciplina, quella introdotta dalla Direttiva 95/46 che, sebbene migliorabile e non priva di difetti, ha costituito uno strumento normativo unico nel suo genere, mediante il quale l'UE è riuscita ad imporre, sulla scena internazionale, un vero e proprio standard europeo in materia di tutela dei dati personali[251].

Ne é testimonianza il fatto che numerosi Stati non facenti parte dell'Unione Europea, quali Canada, Norvegia, Giappone, Israele ed Australia hanno provveduto a riformare la propria normativa interna in materia di protezione dei dati personali al fine di riavvicinarsi allo standard europeo. Allo stesso modo, come già evidenziato anche da questo lavoro, il sistema normativo introdotto a seguito della Direttiva 95/46 ha determinato l'avvio di un dibattito anche negli Stati Uniti, dibattito che sta portando ad un vero e proprio ripensamento circa le modalità attraverso le quali il common law e le leggi americane dovrebbero tutelare la privacy dei propri cittadini.

2. La scelta del regolamento come strumento di riforma

[250] Cfr. punto 40 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012
[251] Françoise Gilbert, nota 244

Il fatto che la Commissione stesse lavorando alacremente ad un progetto di riforma dell'intera struttura normativa europea in materia di protezione dei dati non ha mai costituito un segreto, come peraltro testimoniato dalla Comunicazione inviata al Consiglio ed al Parlamento Europeo già nel Novembre del 2010. Tuttavia, ciò che probabilmente ha colto di sorpresa i commentatori è stato il lancio di una proposta di regolamento anziché la pubblicazione di una bozza di direttiva[252].

In effetti, balza immediatamente all'occhio l'ambiziosità del progetto di riforma, atteso che la Commissione si propone niente meno che di sostituire la vigente disciplina mediante l'adozione di un regolamento che, notoriamente, rappresenta il mezzo privilegiato ogniqualvolta le istituzioni europee si propongono di raggiungere un obiettivo di uniformazione legislativa all'interno dell'Unione.

Il regolamento ha, infatti, una massima incidenza sul diritto degli stati membri rispetto alle direttive in quanto, ai sensi dell'art. 288 TFUE esso è immediatamente efficace e trova diretta applicazione all'interno degli ordinamenti nazionali e con precedenza rispetto alla legislazione domestica non compatibile, senza necessità che gli Stati adottino alcun provvedimento interno di recepimento[253].

Al contrario la direttiva, strumento tradizionalmente utilizzato per ottenere l'armonizzazione e il ravvicinamento della legislazioni interne, fissa soltanto un obiettivo di risultato, lasciando agli Stati membri un margine più o meno ampio di discrezionalità circa le modalità interne di trasposizione. Questa tecnica legislativa ha l'indubbio vantaggio di far si che l'adeguamento della normativa interna agli standard europei risulti meno "brusco", consentendo alla fonte europea di essere trasposta in maniera tale risultare più facilmente "assimilabile". Tuttavia, la trasposizione di una direttiva, essendo comunque regolata dall'ordinamento interno di ciascuno Stato membro, conduce per antonomasia a leggi di attuazione che, sebbene ispirate a principi comuni e a comuni standard di tutela, risultano essere inevitabilmente diverse tra loro[254].

Alla luce di quanto ora detto appare evidente che la Commissione, mediante l'adozione di un Regolamento, mira ad assicurare, sul territorio dell'Unione Europea, la vigenza di un'unica disciplina normativa uguale per tutti gli Stati.

In quest'ottica, il progetto di riforma si propone di eliminare uno dei principali intralci che caratterizzano la disciplina vigente e di cui si è già avuto modo di parlare nei precedenti capitoli di questa tesi, ossia quello della diversità con la quale gli Stati membri hanno

[252] Idem
[253] G. Strozzi, nota 142 p. 310 e ss.
[254] Gianantonio Benacchio "*Diritto Privato della Comunità Europea. Fonti, modelli, regole*", Cedam 2004 p. 178

provveduto a dare attuazione alla Direttiva 95/46, situazione che ha creato sotto molteplici aspetti disomogeneità ed incertezza giuridica per aver dato vita ad un sistema di protezione che varia in funzione del diritto di ciascuno dei 27 Stati che compongono l'Unione Europea. Certo, non bisogna pensare che, con il futuro Regolamento, l'uniformazione sarà totale. E' stato acutamente osservato, infatti, che le autorità amministrative e giudiziarie degli Stati membri continueranno, anche sotto la vigenza della nuova normativa, ad avere una propria interpretazione delle norme[255]. Tuttavia, pare ragionevole attendersi che le differenze tra le interpretazioni risulteranno meno significative rispetto al sistema attuale.

In ogni caso, sebbene la scelta della Commissione di ricorrere ad un regolamento sia stata generalmente accolta con favore da parte della dottrina e degli organismi istituzionali europei, tra cui il Garante Europeo per la protezione dei dati - che ha salutato l'iniziativa come "*un enorme passo avanti nella protezione dei dati personali in Europa*"[256]- non sono tuttavia mancate delle manifestazioni di perplessità con riguardo alla scelta operata dalla Commissione.

E' questo il caso del Comitato Economico e Sociale il quale nel suo parere[257], sebbene abbia riconosciuto i vantaggi e gli aspetti positivi necessariamente sottesi all'adozione di un regolamento in questa delicata materia, si è comunque posto il problema dell'opportunità di tale scelta.

In particolar modo, il Comitato Economico e Sociale ha ritenuto che la Commissione dovesse giustificare meglio, anche alla luce del principio di sussidiarietà, le ragioni in fatto ed in diritto poste a fondamento dell'adozione di uno strumento normativo altamente "invasivo" quale è appunto il Regolamento, in maniera tale da evidenziare analiticamente i motivi che hanno spinto la Commissione a ritenerne preferibile, se non indispensabile, l'adozione rispetto ad una direttiva.

In egual misura, il Comitato Economico e sociale ha espresso la sua perplessità di fronte alla scelta di sottrarre agli Stati membri qualsiasi prerogativa di discrezionalità con riguardo all'attuazione della normativa[258]. Si tratta di una preoccupazione, questa, che non è sfuggita neppure al Garante Europeo per la protezione dei dati, il quale pure ha osservato come, nonostante il regolamento sia comunque lo strumento preferibile, sarebbe stato comunque opportuno lasciare agli Stati membri un certo margine per adottare delle normative nazionali

[255] Françoise Gilbert, nota 244
[256] Comunicato Stampa del 25 gennaio 2012 del Garante Europeo per la Protezione dei Dati, reperibile sul sito www.epds.europa.eu
[257] Punto 1.2 del Parere del Comitato Economico e Sociale, reperibile al sito http://www.eesc.europa.eu/?i=portal.en.soc-opinions.22438
[258] V. punto 4.6 del Parere del Comitato Economico e Sociale

al fine di incorporare le disposizioni del Regolamento, ovvero dettare specifiche norme che possono essere giustificate per determinate aree in cui vi sono delle differenze culturali tra Stati membri[259].

A parere di chi scrive, i dubbi espressi dal Comitato Economico e Sociale e, per certi versi, anche dal Garante Europeo per la protezione dei dati, sono tutt'altro che infondati e questo per almeno due buone ragioni. In primo luogo, infatti, la normativa concernente la tutela ed il trattamento dei dati personali si caratterizza per essere una disciplina altamente tecnica. In quest'ottica, dunque, ci si può e si deve domandare se la Commissione sarà davvero in grado, mediante un unico strumento normativo, di puntare all'integrale sostituzione, oltre che del sistema inaugurato dalla Direttiva 95/46, anche delle legislazioni maturate dai 27 Stati membri nel corso di quasi due decenni. Sotto quest'ottica, lo sforzo della Commissione si profila alquanto titanico in quanto l'iter legislativo dovrà necessariamente portare al licenziamento di un testo sufficientemente dettagliato.

In secondo luogo, l'elevato tecnicismo della materia, combinato con la diretta applicabilità della nuova normativa, rende particolarmente sentito il problema linguistico in quanto il Legislatore dovrà aver cura di assicurare l'esatta corrispondenza delle traduzioni del testo in tutte le lingue nazionali al fine di evitare problemi di applicazione.

Ciò premesso, il Comitato Economico sociale ha altresì sottolineato come la vigenza della Direttiva 95/46 si sia protratta per oltre sedici anni. Di conseguenza gli Stati membri, mediante l'emanazione delle normative nazionali di attuazione della direttiva, unitamente all'evoluzione della giurisprudenza domestica ed all'azione costante delle autorità di vigilanza hanno maturato un'esperienza significativa in tema di tutela dei dati personali. In quest'ottica il Comitato Economico e Sociale non appare completamente convinto dell'opportunità di travolgere tale esperienza e, per tale motivo, evidenzia l'opportunità di lasciare gli Stati membri la libertà di poter adottare delle disposizioni nazionali sia nelle aree non coperte dalla proposta normativa, sia disposizioni maggiormente favorevoli rispetto a quelle contenute nel Regolamento. Senza contare poi l'esigenza, sottolineata sempre dal Comitato Economico e Sociale, di garantire la vigenza quelle normative nazionali che già attualmente prevedono un livello di tutela maggiore rispetto a quello contenuto nella proposta della Commissione.

Infine, il Comitato Economico e Sociale non ha mancato di rilevare un altro punto controverso del progetto di riforma. Le 118 pagine che compongono l'attuale versione del testo licenziato dalla Commissione sono tempestate di riferimenti all'esercizio dei poteri delegati ex art. 290 TFUE. Invero, trattandosi come si è detto di materia particolarmente

[259] Cfr. punto 64 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012

tecnica, era del tutto scontato che la Commissione non sarebbe mai stata in grado di esaurire l'intera materia con un colpo solo, dovendo comunque riservarsi la possibilità di intervenire successivamente mediante l'emanazione di " *atti non legislativi di portata generale al fine di integrare o modificare determinati elementi non essenziali*" del Regolamento stesso. Tuttavia, il Comitato Economico e Sociale, nel prendere atto di tali numerosi riferimenti all'esercizio dei poteri delegati, rileva di non poter ritenere accettabili quelli che non rispecchiano i parametri stabiliti dall'art. 290 TFUE che disciplina le condizioni di legittimità per l'esercizio dei poteri delegati.

Il Comitato Economico e Sociale ha rilevato, infatti, come la disciplina di molti aspetti cruciali del regolamento nonché di diversi elementi inerenti al funzionamento del relativo meccanismo di tutela sia stata demandata a futuri atti delegati. Correttamente, dunque, il Comitato evidenzia che tale tecnica legislativa non può ritenersi compatibile con i limiti stabiliti dall'art. 290 TFUE con pesanti ricadute sulla certezza legale del testo.

Anche a parere del Garante Europeo per la protezione dei dati[260]sarebbe stato opportuno evitare un così massiccio ricorso ai poteri delegati, ravvisando la necessità che i temi attualmente oggetto di alcune specifiche deleghe vengano affrontati direttamente dal Legislatore.

Sotto questo profilo il Garante osserva che, nel caso in cui gli atti delegati non siano adottati nel momento di entrata in vigore del Regolamento (cosa che pare peraltro alquanto probabile con riferimento alla maggioranza degli atti delegati previsti), l'efficace applicazione del regolamento potrebbe essere a rischio. Tale potrebbe essere, ad esempio, il caso del sistema sanzionatorio previsto dall'art. 79 della Proposta di Regolamento. Infatti, un sistema sanzionatorio uniforme all'interno dell'Unione Europea dipende necessariamente dall'esistenza di sufficiente chiarezza circa il significato preciso delle norme applicabili, necessariamente precisato da atti delegati o attuativi. Per esempio, se il mancato rispetto del tempestivo obbligo di notificare gli accessi non autorizzati alle banche dati contenenti informazioni personali può essere sanzionato con un importo sino ad un milione di Euro, senza una norma che precisi chiaramente quale sia la soglia sanzionatoria applicabile caso per caso, le varie prassi nazionali potrebbero risultare grandemente difformi, con gravi conseguenze per il funzionamento del mercato interno.

Allo stesso modo, nell'ottica del Garante Europeo[261] non appare affatto scontato che gli atti delegati contemplati dalla proposta di Regolamento siano tutti "limitati ad elementi non

[260] Cfr. punto 71 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012
[261] Cfr. punto 74 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012

essenziali" così come stabilito dall'art. 290 TFUE. Anche qui, il meccanismo che disciplina la notificazione della *personal data breach* costituisce un elemento essenziale che, anziché essere devoluto ad un atto delegato, dovrebbe invece essere disciplinato direttamente dal regolamento. Secondo il Garante Europeo, dunque, l'uso di nozioni vaghe non può giustificare l'attribuzione alla Commissione di poteri pressoché illimitati di adottare atti delegati. La certezza del diritto richiede, al contrario, che queste nozioni siano sufficientemente definite nel testo legislativo.

In altre parole gli organi consultivi paiono lamentare una eccessiva concentrazione di poteri nelle mani della Commissione a detrimento del principio di sussidiarietà e della certezza del diritto. Ed è prevedibile che tali lacune verranno sicuramente evidenziate anche dal Parlamento Europeo.

Un altro punto controverso della proposta di riforma riguarda le numerose eccezioni e deroghe ai diritti ivi contemplati. Invero, il Comitato Economico e sociale ha avuto modo nel suo parere di lamentare la sussistenza di numerose deroghe ed eccezioni rispetto ai diritti individuali riconosciuti[262]. In particolar modo, numerose ed eccessivamente ampie sono le deroghe previste per le micro, piccole e medie imprese, che di fatto dispensano queste ultime da numerosi adempimenti tra cui quello di nominare un *data protection officer*. A ben vedere, inoltre, ogniqualvolta il Regolamento autorizza la Commissione ad adottare atti delegati o attuativi viene molto spesso affermato che la medesima adotterà le misure appropriate o specifiche per le PMI.

In realtà, sebbene sia comprensibile che la differenza in termini di dimensioni di un'impresa possa avere un effetto sul perso degli oneri amministrativi addizionali che derivano dalle regole sulla protezione dei dati, si deve tuttavia osservare come la protezione dei dati costituisca un diritto fondamentale e che, pertanto, gli individui hanno diritto allo allo stesso livello di protezione dei loro dati a prescindere dal fatto che questi vengano trattati da un'impresa di piccole dimensioni ovvero da grosse realtà societarie.

Un altro punto debole del pacchetto di riforma annunciato dalla Commissione è dato dalla sua mancanza di omogeneità. Si tratta di una debolezza rilevata dal Garante Europeo della Protezione dei Dati il quale osserva che, al di là della scelta criticabile di adottare un separato strumento normativo per quanto riguarda il trattamento di dati personali nel settore della cooperazione di polizia e giudiziaria di cui si è già parlato, la futura riforma interesserà soltanto parzialmente il quadro legislativo in materia di protezione dei dati[263].

[262] Punto 3.2 del Parere del Comitato Economico e Sociale
[263] Cfr. punto 80 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012

Invero, la disciplina riguardante la protezione dei dati per le istituzioni dell'UE, organi e agenzie così come contenuta nel Regolamento n. 45/01 è rimasta invariata, al pari di specifici provvedimenti, quali le regole per Europol ed Eurojust o le regole sulla protezione dei dati ai sensi della decisione di Prum. Allo stesso modo non vi sono regole prevedibile per la Politica Estera e di Sicurezza Comune ai sensi dell'art. 39 TUE. E' per questo motivo che il Garante Europeo ritiene necessario inglobare le disposizioni del Regolamento 45/01 nella nuova proposta, sul presupposto che singoli testi normativi evitano il rischio di discrepanze tra le rispettive disposizioni.

In subordine, osserva il Garante, la Commissione dovrebbe impegnarsi al fine di assicurare che le regole che valgano per le istituzioni e gli organi dell'UE siano allineate alla nuova proposta generale di regolamento, dal momento in cui non sarebbe accettabile che le istituzioni europee possano non essere vincolate da una normativa che trova applicazione nei confronti degli stati membri[264].

In ogni caso, al di là di queste considerazioni di carattere tecnico il complesso della dottrina e delle istituzioni e degli organi consultivi dell'Unione Europea sembra avere accolto con decisivo favore la proposta di regolamento, ritenendo quest'ultimo come lo strumento privilegiato e maggiormente idoneo per riformare l'edificio normativo europeo sulla protezione dei dati personali.

3. Le principali novità introdotte dalla riforma

Come si accennava nei paragrafi precedenti la proposta di regolamento della Commissione Europea ha come primario obiettivo quello di rafforzare la protezione dei dati personali quale diritto fondamentale, nonché quello di consolidare e promuovere il mercato interno legato ai servizi digitali. Sotto questo profilo la riforma introduce delle nuove ed importanti novità che si provvederà ad analizzare a grandi linee in questa sede.

Innanzitutto, già la scelta dello strumento normativo per la realizzazione della riforma, ossia **il regolamento**, costituisce di per sé una novità. Infatti, come si diceva poc'anzi l'eliminazione delle difformità con le quali gli Stati membri hanno recepito la vecchia direttiva avrà come effetto quello di comportare, oltre che una semplificazione della normativa ed una maggiore certezza del diritto, anche un notevole risparmio in termini di

[264] Cfr. punto 68 del Parere del Garante Europeo per la Protezione dei Dati Personali del 7 Marzo 2012

minori costi amministrativi e burocratici sia per le aziende private che per le amministrazioni statali.

In particolare la Commissione stima che la semplificazione normativa possa portare ad un risparmio annuale di 2,3 miliardi di Euro per le aziende, nonché rinforzare la fiducia dei cittadini nei confronti dei servizi online ai fini della promozione del mercato unico digitale[265]. Ciò dovrebbe avere come ulteriore effetto, altresì, quello di incentivare la crescita economica, creare nuovi posti di lavoro ed allentare le barriere che attualmente inibiscono una piena risposta europea all'attuale crisi economica.

Secondo l'intento della Commissione, dunque, l'uniformazione della normativa stimolerà soprattutto le piccole-medio imprese, attualmente disincentivate dai costi e dalle incertezze derivanti dalla disomogeneità della vigente normativa, a varcare i confini nazionali per offrire i propri servizi sul territorio di altri Stati membri. Allo stesso modo la presenza di una normativa univoca e coerente potrebbe altresì attrarre la presenza di realtà aziendali di grosse dimensioni ed incoraggiare gli investimenti dall'estero[266].

Su di un versante parallelo, poi, il progetto di riforma mira a rafforzare la fiducia dei cittadini europei nei confronti dei servizi online, garantendo loro un maggiore controllo ed una maggiore sicurezza circa il trattamento dei loro dati, pur nell'ambito di un contesto normativo semplificato. L'Eurobarometro, infatti, ha evidenziato come le preoccupazioni che ruotano intorno alla tutela della privacy si collocano ai primi posti tra le ragioni che spingono i consumatori a diffidare dei servizi online[267]. Orbene, nell'ottica della Commissione, la consapevolezza che i propri dati verranno trattati con eguale scrupolo e con lo stesso standard di protezione in tutti gli stati membri dovrebbe incentivare il ricorso alle transazioni via internet da parte dei cittadini.

Ciò premesso, il regolamento semplifica di non poco gli oneri amministrativi attualmente gravanti sulle aziende. In particolar modo viene prevista **l'eliminazione degli obblighi di notifica.**

Infatti, ai sensi dell'attuale disciplina le aziende che raccolgono dati personali sono tenute a notificare le suddette attività alle autorità di vigilanza di ciascuno Stato membro. Si tratta, con ogni evidenza, di un obbligo particolarmente gravoso soprattutto per quelle realtà

[265] Cfr. comunicato stampa della Commissione consultabile sul sito http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm

[266] Cfr. Commissione Europea "*How will the EU data protection reform strengthen internal market*" , reperibile su http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/4_en.pdf

[267] Risultati del sondaggio Eurobarometer sono consultabili alla pagina ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

aziendali di grosse dimensioni che operano su scala europea, le quali sono tenute ad effettuare detta operazione nei confronti delle autorità di ciascuno Stato membro presso cui operano.

Orbene, il regolamento abolisce siffatto obbligo di preventiva notifica, stabilendo che le aziende dovranno provvedere a dotarsi di un'efficiente organizzazione interna (è previsto ad esempio che le aziende che superino i 250 dipendenti nominino un *data protection officer*) al fine di conservare la documentazione pertinente ai trattamenti di dati personali nonché quant'altro sia necessario in caso di controllo o ispezione da parte dell'autorità di vigilanza statale competente con la quale dovranno cooperare.

Si passa così da un sistema di controllo preventivo, ad un sistema di controllo successivo meramente eventuale che si fonda, tuttavia, su di una maggiore responsabilizzazione degli enti privati (principio di responsibility e accountability) nonché nella previsione dell'obbligo di dotarsi di una struttura interna efficiente per il trattamento dei dati ("data protection by design"). Sulla scia di questi principi viene ad esempio previsto che le imprese dovranno notificare all'autorità di vigilanza non appena possibile, possibilmente entro 24 eventuali "data breach", ossia intrusioni non autorizzate nelle banche dati suscettibili di mettere in pericolo le informazioni personali ivi custodite.

Ma vi è di più.

Il regolamento stabilisce, inoltre, che le aziende saranno soggette all'autorità di controllo esclusiva dell'Autorità di vigilanza dello Stato membro nel cui territorio hanno la loro sede amministrativa. Inutile dire che tali cambiamenti semplificheranno notevolmente la vita delle imprese e comporteranno altresì una significativa riduzione dei costi scongiurando, altresì, i rischi di "forum shopping". In quest'ottica la Commissione stima che la riforma comporterà un risparmio annuo di oltre 130 milioni di Euro[268].

Su di un versante parallelo, poi, il regolamento accresce notevolmente i poteri di controllo da parte delle autorità di vigilanza a livello statale. In particolare, è previsto che, in caso di violazione degli obblighi derivanti dal regolamento, le stesse potranno irrogare alle aziende inadempienti delle sanzioni sino al 2% del fatturato annuo ovvero fino a 1 milione di euro. Si tratta, evidentemente, di un'innovazione destinata ad uniformare una prassi, quella attuale, profondamente difforme e caratterizzata dall'irrogazione di sanzioni particolarmente basse o poco dissuasive[269]. In quest'ottica, dunque, il regolamento lancia un segnale preciso, ossia quello di perseguire in maniera più aggressiva le infrazioni e di equipaggiare le autorità di vigilanza con sostanziali strumenti volti ad assicurare il rispetto della legge

[268] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=en&guiLanguage=en

[269] Françoise Gilbert, nota 244

Sul versante dei diritti individuali invece, giova premettere come sebbene sia la direttiva che la proposta di regolamento perseguano la protezione dei dati e la libera circolazione di tali dati come loro obiettivi essenziali, l'art. 1 della Direttiva 95/46 dispone che gli Stati membri proteggono "*i diritti fondamentali e le libertà delle persone fisiche* ***in particolare il loro diritto alla privacy*** *con rispetto al trattamento dei dati personali*", mentre al contrario gli artt. 1 e 2 del Regolamento prevedono tra i propri obiettivi la necessità di "*proteggere il diritto fondamentale e le libertà delle persone fisiche* ***in particolare il loro diritto alla protezione dei dati personali***".

Con ogni evidenza nella proposta di regolamento la protezione dei dati personali viene in qualche modo sganciata dalla protezione della privacy. Allo stesso modo, secondo attenta dottrina, la parola privacy di per sé "*appare completamente espunta dal nuovo testo normativo e compare assai meno frequentemente nella proposta di regolamento di quanto non accada invece nella direttiva*"[270]. Alla luce delle considerazioni che precedono, pertanto, diversi commentatori si sono chiesti se questo cambiamento nello stile di redazione del testo normativo segni un passo decisivo verso una definitiva autonomizzazione del concetto di tutela dei dati personali rispetto alla più ampia e generica tutela della privacy[271]. In effetti tale dissociazione non è nuova nel panorama normativo dell'Unione Europea giacché già in seno alla Carta dei Diritti fondamentali dell'Unione Europea, la tutela dei dati personali prevista dall'art. 8 viene contemplata in una disposizione separata rispetto alla tutela della vita privata.

Tuttavia, parte della dottrina ha ravvisato in siffatta distinzione, più che una novità, un vero e proprio pericolo per le libertà individuali[272], in quanto avrebbe come potenziale effetto quello di sottrarre il Regolamento alla sfera di applicazione della giurisprudenza della Corte Europea dei Diritti Umani. In altri termini, secondo questa parte della dottrina bisognerebbe rafforzare, anziché recidere il legame intrinseco tra privacy e protezione dei dati personali, che in una società rappresenta una *condicio sine qua non* per il godimento delle altre libertà civili piuttosto che una finalità in sé[273].

Allo stesso modo, sempre con riferimento al contenuto del Regolamento, il Comitato Economico e sociale ha avuto modo di rilevare come esso avrebbe potuto spingersi molto più in là nell'incrementare la protezione offerta ad alcune tipologie diritti che, al contrario, risultano indeboliti per effetto della previsione di una moltitudine di eccezioni e di deroghe[274],

[270] Idem
[271] Luis Costa, Yves Poullet, nota 236
[272] Idem
[273] Ioannis Ntouvas *"Single new law to reform data protection proposed by European Commission"* Journal of Computer, Media & Telecommunications Law; 2012 vol 17 issue 1, p. 3-4
[274] Cfr. punto 3.9 del Parere del Comitato Economico e Sociale

non da ultimo quelle riguardanti le piccole e medie imprese di cui si è già detto. Ad esempio, osserva il Comitato Economico e Sociale, la nozione di interesse pubblico nel Regolamento viene costruita al fine di legittimare vere e proprie deroghe rispetto ai principi generali. Tuttavia, una definizione precisa del concetto di interesse pubblico risulta assente nel testo normativo[275], che propende per una nozione ampia. In quest'ottica, dunque, il Comitato Economico e Sociale ritiene che sarebbe stato necessario un maggiore bilanciamento tra i diritti delle parti interessate, al fine di scongiurare il rischio di sacrificare le esigenze di tutela del diritto fondamentale alla protezione dei dati in favore degli interessi del mercato. Allo stesso modo il Comitato evidenzia come la proposta riguardi soltanto i diritti delle persone fisiche laddove si poteva comunque estendere la protezione anche alle persone giuridiche[276].

Va, inoltre, osservato che da una lettura comparativa delle disposizioni del nuovo Regolamento con quelle della Direttiva, balza immediatamente all'occhio l'avvenuto **rafforzamento del ruolo del consenso individuale**.

Attualmente, infatti, ai sensi la legislazione di molti Stati membri della Ue il consenso è dato per implicito in numerose circostanze[277]. Si ritiene, ad esempio, che un individuo che utilizzi un sito Web abbia necessariamente aderito alla politica sulla privacy di tale medesimo sito, senza necessità che il relativo consenso sia stato manifestato esplicitamente. In altre parole, secondo la disciplina attualmente vigente, salvo per ciò che riguarda il trattamento dei dati sensibili, è sufficiente che il consenso venga manifestato in maniera "*non ambigua*" ergo si ammette la possibilità che lo stesso venga fornito anche per *facta concludentia*[278].

Al contrario, ai sensi del nuovo regolamento, laddove il consenso rappresenti il fondamento per la legittimità del trattamento dei dati, esso dovrà essere specifico ed espresso in maniera esplicita. Si tratta, evidentemente, di una novità diretta a garantire un maggiore controllo, da parte dei cittadini, dei propri dati personali in quanto sarà onere da parte dei responsabili del trattamento non soltanto quello di renderli edotti della specifica natura e delle finalità del trattamento, ma anche di richiedere il loro consenso esplicito all'operazione.

Sotto questo profilo, dunque, si avrà una vera e propria inversione dell'onere della prova, giacché il responsabile del trattamento dovrà fornire la dimostrazione che il titolare dei dati aveva dato il suo consenso esplicito al trattamento dei medesimi per specifiche finalità. Tutto questo farà si che le aziende che hanno raccolto le informazioni personali relative ad individui

[275] Cfr. punto 4.19 del Parere del Comitato Economico e Sociale
[276] Cfr. Punto 2.1 del Parere del Comitato Economico e Sociale
[277] Françoise Gilbert, nota 244
[278] Ioannis Ntouvas, nota 273

dovranno recuperare prova del consenso ricevuto e, in caso di dubbio, richiederlo nuovamente.

Di particolare rilevanza, poi, sempre in chiave di rafforzamento del consenso è l'art. 7 par 4 del Regolamento che recita che "il *consenso non costituirà un fondamento legale per il trattamento ove vi sia uno squilibrio significativo tra la posizione del titolare dei dati e quella del responsabile del trattamento*".

In effetti l'asimmetria informativa che generalmente permea tutte le operazioni di raccolta e trattamento dei dati è stata il motivo principale che ha motivato l'affermazione, sempre da parte del Regolamento, del **principio di trasparenza.** Invero i cittadini sono raramente consapevoli delle modalità attraverso cui i loro dati vengono raccolti e trattati mentre navigano Internet, utilizzano i loro cellulari ovvero camminano lungo una strada video-sorvegliata[279]. La legislazione sulla tutela dei dati personali deve avere dunque tra le proprie finalità quella di correggere tale asimmetria, contro bilanciando la forza di governi e industria al fine di proteggere i cittadini. In quest'ottica il principio di trasparenza mira a creare un'aura di fiducia attorno alle operazioni di trattamento dei dati personali.

Il rafforzamento del consenso deve essere letto unitamente alla possibilità, introdotta sempre dal regolamento, di azioni collettive a tutela dei dati personali. In particolare, accanto alla tradizionale tutela giudiziaria ed amministrativa già prevista in favore del singolo, il regolamento affianca una sorta di **tutela collettiva**, che si traduce nella possibilità per associazioni di consumatori e organizzazioni non governative di proporre dei ricorsi collettivi sia a livello giudiziale che amministrativo.

Sempre con riferimento ai diritti individuali, la proposta di regolamento circoscrive notevolmente la quantità di dati sottoponibili a trattamento, introducendo un vero e proprio **principio di limitazione dei dati**. Infatti, se la direttiva afferma che i dati non devono essere "*eccessivi rispetto lo scopo perseguito"*, il regolamento dispone invece che "***essi devono essere limitati al minimo****"*. Si tratta, evidentemente, di una novità diretta a rafforzare la fiducia nei confronti della *digital economy*, posto che secondo l'Eurobarometro[280] due terzi dei cittadini europei, oltre a temere il fatto che i dati raccolti, soprattutto online, possano essere utilizzati per finalità diverse da quelle che ne hanno giustificato il trattamento, lamentano di sentirsi costretti a fornire più dati personali di quanti non stimino realmente necessario.

[279] Idem

[280] Risultati del sondaggio sono consultabili alla pagina ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

Detto principio deve essere letto in combinazione con un altro nuovo concetto introdotto dalla nuova normativa, ossia quello del "**privacy by default**". Tale nozione implica che le impostazioni "standard" di qualsiasi servizio che implica la raccolta e il trattamento di dati personali debbano essere quelle che assicurano un maggiore livello di tutela della privacy.

Un'altra novità di cui si è discusso a lungo in dottrina riguarda il "**diritto all'oblio**" ossia il diritto di ciascun cittadino a che i propri dati personali vengano cancellati su sua espressa richiesta dopo un determinato periodo di tempo e nel caso in cui non vi siano ragioni imperative che ne giustifichino la raccolta.

In un epoca caratterizzata dall'imperversare dei social network il diritto all'oblio si configura come un'ulteriore garanzia della privacy individuale intesa come diritto fondamentale che si pone come condizione per la fruibilità di ulteriori diritti primari, non da ultimo il diritto allo sviluppo della propria personalità.

In quest'ottica gli utenti potranno chiedere ed ottenere la cancellazione di informazioni personali, fotografie e quant'altro sia stato pubblicato sui social network, che stimeranno non essere più in linea con l'evoluzione del proprio pensiero e della propria personalità. Ciò costituirà un ulteriore strumento per l'auto-protezione dei cittadini dai rischi legati alla circolazione e, soprattutto alla permanenza, di proprie informazioni personali sulla rete, nonché contro il rischio di uso distorto di informazioni passate. Proprio per questi motivi il regolamento afferma che il diritto all'oblio assume una speciale rilevanza ove l'individuo abbia reso disponibile tale dati quando era minore d'età.

Infatti, le disposizioni relative al diritto all'oblio sono strutturate in maniera tale da prevedere un'inversione dell'onere della prova: una volta inoltrata la richiesta di cancellazione, infatti, saranno i responsabili del trattamento, e non l'utente,a dover provare che il mantenimento delle informazioni è giustificato da ragioni legittime.

Il diritto all'oblio dunque amplifica l'efficacia della protezione dei dati nei suoi principi e regole. Per esempio mentre la direttiva permette alle persone di cancellare dati soltanto quando non vi sia rispetto della legge, il nuovo regolamento permette altresì agli individui il diritto di ottenere la cancellazione laddove essi abbiano ritirato il loro consenso, circostanza questa che rappresenta un chiaro incremento del potere di controllo da parte degli utenti..

Ciò premesso, sempre nell'ottica di incentivare i servizi legati alla *digital economy* la proposta di regolamento varata dalla Commissione introduce il concetto di **"portabilità dei dati personali**". Si tratta di una novità che comporterà il diritto per ciascun cittadino di ottenere una sorta di "backup" dei dati personali raccolti da un internet service provider e di trasferirli in blocco verso un altro internet service provider. Da un punto di vista giuridico

questa novità, unitamente al rafforzamento della disciplina del consenso, comporterà per i cittadini un maggiore controllo circa la natura e della tipologia dei dati che vengono attualmente raccolti e gestiti dai *providers*

Chiaramente, scopo della riforma in questo senso è quello di stimolare la competitività degli operatori, incoraggiandoli a fornire servizi economicamente efficienti a beneficio del consumatore finale.

CAPITOLO IV

PARTE PRIMA

"LA DIMENSIONE ESTERNA DELLA TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA"

1. Considerazioni generali

Questo capitolo verrà dedicato all'analisi della "dimensione esterna" della tutela dei dati personali nell'ordinamento giuridico dell'Unione Europea. In altri termini, verranno illustrati in questa sede i principi e gli strumenti normativi attraverso i quali l'Unione Europea si propone di assicurare ai dati personali che fuoriescono dal suo territorio un elevato livello di protezione, il più possibile vicino allo *standard* di tutela vigente all'interno dei suoi confini.

Preliminarmente si deve osservare come, per qualsiasi giurista tradizionale, il concetto di "dimensione esterna", riferito ad un contesto normativo interno, possa destare qualche perplessità. La legge, infatti, salvo alcuni casi tassativamente individuati di applicazione extra-territoriale, è generalmente soggetta a dei rigidi criteri di applicazione spazio-temporale – in modo tale da risultare applicabile soltanto a fatti successivi alla sua entrata in vigore e nei limiti dei confini statali-. In un'ottica tradizionale, quindi, il concetto di dimensione "esterna", riferito alla tutela dei dati personali, può apparire come una vera e propria *contradictio in terminis*.

In realtà, come si è già visto nei capitoli precedenti, la tutela dei dati personali costituisce, per l'ordinamento giuridico europeo, un vero e proprio diritto fondamentale dell'individuo. Detta concezione é espressione di un'esperienza storico-giuridica e di una sensibilità culturale tipicamente europea, e contraddistingue l'ordinamento dell'Unione rispetto alle tradizioni giuridiche di altre democrazie occidentali, Stati Uniti *in primis*.

Orbene, la tutela di tale diritto fondamentale esige che i dati personali, che presentano la particolarità addizionale di poter essere messi in circolo con estrema facilità e di poter fuoriuscire dal territorio degli Stati membri con un semplice *click* del mouse, debbano essere protetti non soltanto quando circolano all'interno del territorio dell'Unione, ma anche nel caso in cui vengano trasferiti all'estero. Viceversa, infatti, sarebbe sufficiente trasferirli e sottoporli a trattamento in un Paese esterno all'Unione Europea, col risultato di aggirare le garanzie e di vanificare la legislazione a tutela di tale diritto fondamentale.

Ora, il concetto di dimensione "esterna" della tutela dei dati personali mira a dare una risposta a questa esigenza di protezione. La direttiva 95/46/CE in materia di tutela dei dati personali ha, infatti, disposto espressamente la propria applicazione (cfr. art. 4) anche ai "*responsabili dei trattamenti di dati personali*", a coloro cioè che "*determinano le finalità e gli strumenti del trattamento di dati personali*", anche se non stabiliti nel territorio della Comunità, quando ricorrano a strumenti, automatizzati o meno, situati nel territorio di uno Stato membro e purché non servano solo a fini di transito delle informazioni nel territorio della Comunità.

Allo stesso modo, al fine di assicurare appieno la tutela delle singole persone i cui dati siano trattati in Europa, la direttiva contiene disposizioni specificamente dedicate al trasferimento dei dati dall'Unione europea verso altri Paesi, prevedendo norme sia sostanziali che procedurali tese a innalzare il tenore internazionale della protezione delle persone da abusivi trattamenti dei loro dati personali[281]; queste disposizioni hanno conosciuto un importante contributo interpretativo-specificativo da parte di un apposito organo, il "Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali" (qui di seguito, il "Gruppo").

Invero, come si vedrà in proseguo, la Direttiva 95/46/CE contiene un intero capo dedicato alla disciplina dei trasferimenti di dati personali verso Paesi terzi. Lo spirito della direttiva, infatti, così come espresso ai considerando nn. 56 e 57, è quello di proibire il trasferimento di dati personali allorquando lo Stato destinatario del flusso di dati non offra un adeguato livello di protezione e, viceversa, di consentirlo, soltanto laddove lo stato terzo di destinazione assicuri, invece, detto *standard* di tutela. In altre parole, l'ordinamento giuridico dell'Unione Europea mira ad assicurare che i dati personali dei propri cittadini continuino a beneficiare di un elevato standard di protezione anche nell'ipotesi in cui lascino il territorio degli Stati membri.

Secondo attenta dottrina le ragioni dell'influenza esterna della politica europea in materia di tutela dei dati personali sono duplici[282]. Da un lato, infatti, il carattere globale del commercio e delle relazioni umane transitante sulle reti telematiche rende oramai vano qualsiasi tentativo di offrire una protezione efficace dei dati attraverso iniziative meramente unilaterali. Sull'opposto versante, invece, vi è l'esigenza di evitare che i flussi di dati vengano intralciati dall'esistenza di difformità normative ed incertezze giuridiche. Non si deve dimenticare, sotto questo aspetto, che la Direttiva 95/46/CE nasce essenzialmente con l'obiettivo di assicurare la libera circolazione dei dati all'interno del territorio europeo nell'ottica del migliore funzionamento del mercato comune.

[281] Paolo Pallaro, "*Rapporti Commerciali tra UE e Stati Terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA*", in Diritto del Commercio internazionale 2000,03,753
[282] Idem

Ciò premesso, sempre secondo quanto osservato da una parte della dottrina[283], l'introduzione di disposizioni tali da consentire l'applicazione extraterritoriale della direttiva sulla protezione dei dati a paesi non europei dimostra inequivocabilmente come l'Unione Europea abbia iniziato ad assumere un ruolo più forte a livello globale a seguito della maggiore integrazione degli Stati membri. Invero, sarebbe alquanto difficile ipotizzare che il singolo Stato membro possa avere da solo la forza di imporre ai propri *partners* internazionali l'adeguamento a standard di protezione puramente interni. Questo risultato diventa, però, conseguibile grazie al maggiore peso cha l'Unione Europea detiene sulla scena internazionale allorquando è in grado di parlare con un'unica voce.

Come si è anticipato, infatti, la legislazione dell'Unione Europea in materia di *data protection* esige che gli Stati terzi destinatari dei flussi di dati forniscano delle garanzie precise volte ad assicurare agli individui un livello di protezione adeguato, pena il divieto di qualsiasi trasferimento di dati, indi l'imposizione di quello che è stato efficacemente indicato come un vero e proprio "embargo" di informazioni[284]. In quest'ottica, quello che viene definito dalla dottrina come "unilateralismo CE" ha conseguito dei risultati sorprendenti per quanto riguarda numerosi paesi non facenti parte dell'Unione Europea, tra i quali il Canada, la Svizzera, il Giappone e l'Australia, i quali hanno spontaneamente adeguato le proprie legislazioni nazionali in materia di *data protection* proprio al fine di allinearsi allo standard di protezione stabilito dalla Direttiva 95/46/CE[285].

Allo stesso modo è stato osservato come, se era tradizionalmente la posizione di egemonia economica americana a creare «esternalità» che richiedevano agli altri Stati risposte politiche per difendersi dall'impatto extraterritoriale degli strumenti di politica interna USA, ora «*the reversal of this pattern has not gone unnoticed*[286]»

Il contenzioso relativo ai PNR, dal canto suo, ha dimostrato invece come l'Unione Europea non sia riuscita a conseguire il medesimo brillante risultato con riguardo alla superpotenza USA, sebbene la vicenda abbia avuto come effetto quello di innescare un vivace dibattito in seno alla dottrina ed all'opinione pubblica d'oltre oceano. Se inizialmente, infatti, la dottrina americana ha ritenuto inammissibile il tentativo da parte dell'Unione Europea di imporre ai propri *partners* commerciali degli standard di protezione della privacy basati su esperienze storiche e concezioni

[283] Ryan Lowther, "*U.S. Privacy Regulations Dictated by EU Law: How the Healthcare Profession May be Regulated*" in Columbia Journal of Transnational Law 41 no2 435-54 2003
[284] Idem
[285] Lauso Zagato "*Il trasferimento di dati personali verso stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*" in Dir. Comm. Internaz. 2008, 02, 297
[286] C.-J. BENNETT, *Privacy Self-Regulation in a Global Economy: a Race to the Top, the Bottom or Somewhere else?* (Atti delle 22ª Conferenza internazionale sulla privacy e la protezione dei dati personali, Venezia, 28-30 settembre 2000).

culturali non condivise dagli altri Paesi[287], oggi il dibattito sembra maggiormente incentrato sull'opportunità di aumentare il livello di protezione dei dati offerto ai cittadini americani, anche per non lasciare al partner Unione Europea il monopolio della protezione della privacy delle persone fisiche[288]. In quest'ottica, risulta affascinante osservare come, nel silenzio assordante della Costituzione federale e della giurisprudenza della Corte Suprema sul punto, diversi stati americani tra cui la Florida e la California abbiano modificato le proprie costituzioni al fine di introdurre delle disposizioni a tutela della privacy dei propri cittadini.

A parere di chi scrive, dunque, alla luce delle suesposte considerazioni, appare evidente come l'evoluzione della normativa europea in materia di protezione dei dati personali non costituisca un fenomeno isolato o, comunque, privo di una sua logica intrinseca. Al contrario, essa sembra corrispondere ad una scelta di "politica estera legislativa" consapevole da parte dell'Unione Europea, mirante ad "esportare", e finanche ad imporre agli altri membri della comunità internazionale degli standard di protezione propriamente europei in materia di tutela dei dati personali.

Questa lettura sembra trovare conferma anche nell'adozione, durante la seduta del 10 e dell'11 dicembre 2009 del Consiglio Europeo, del **Programma pluriennale sulla giustizia e gli affari interni** meglio conosciuto come Programma di Stoccolma[289]. Si tratta sostanzialmente di un testo che contiene la tabella di marcia per i successivi 5 anni per tutti gli aspetti riguardanti l'area libertà, sicurezza e giustizia, che va dalla promozione dei diritti fondamentali alla politica europea sulla giustizia civile e penale, includendo i capitoli sull'immigrazione e sul diritto d'asilo[290].

Il programma di Stoccolma delinea, infatti, le priorità dell'Unione europea (UE) per lo spazio di libertà, sicurezza e giustizia per il periodo 2010-2014, tenendo conto dei risultati conseguiti dai programmi di Tampere e dell'Aia, e mira ad accogliere le sfide future e a rafforzare lo spazio europeo di giustizia, libertà e sicurezza con azioni concentrate sugli interessi e sulle esigenze dei cittadini[291].

In tale sede il Consiglio Europeo ha stabilito che "*l'Unione deve garantire una strategia globale in materia di protezione dei dati all'interno dell'Unione e nell'ambito delle relazioni con i paesi terzi*", invitando la Commissione "*a proporre una raccomandazione per la negoziazione di*

[287] Santolli Justin "*The Terrorist Finance Tracking Program: Illuminating the shortcomings of the European Union's antiquated data protection directive"* in The Geo. Wash. Int'l L. Rev., 2008, 40,2, p. 563 e ss.
[288] Barbara Crulchfield George; Patricia Lynch, Susan J Marsnik "*US multinational employers: navigating through the "Safe Harbor Principles" to comply with the EU data privacy directive",* in American Business Law Journal 38 no 4 753-83 Summ. 2001
[289] GUUE 4.5.2010 C 115/01)
[290] Consultabile al sito http://www.consilium.europe.eu/uedocs/cms_data/docs/pressdata/it/ec
[291]" *Il programma di Stoccolma sullo Spazio di Libertà Sicurezza e Giustizia*", Int'l Lis., 2010,2,62

accordi in materia di protezione e, se necessario, condivisione dei dati", nonché "*a prendere in esame elementi essenziali per accordi sulla protezione dei dati con paesi terzi".*

In un'ottica più ampia, è previsto che l'Unione Europea dovrà avere una funzione motrice per lo sviluppo e la promozione di norme internazionali in materia di protezione dei dati personali, prendendo come base i pertinenti strumenti europei in materia di protezione dei dati e la Convenzione del Consiglio d'Europa del 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, e per la conclusione di adeguati accordi internazionali bilaterali o multilaterali.

Allo stesso modo il Programma di Stoccolma ribadisce il fatto che "*la protezione dei dati personali è un'attività centrale dell'Unione. È necessario che l'Unione si doti di un quadro normativo coerente per i trasferimenti di dati personali verso paesi terzi". In*oltre è previsto che dovrà essere negoziato e concluso rapidamente un accordo sulla protezione dei dati personali scambiati a fini di contrasto della criminalità.

Nei prossimi paragrafi verranno quindi illustrati i frutti che, nel bene e nel male, la "politica legislativa estera" dell'Unione Europea in materia di *data protection* ha fino ad oggi raccolto (o che avrebbe potuto raccogliere) nell'ottica di garantire ai dati personali dei propri cittadini che fuoriescono dai confini europei un elevato livello di protezione.

2. La disciplina dei trasferimenti di dati personali all'estero e la nozione di livello adeguato di protezione

Notoriamente il pilastro principale della legislazione europea in materia di protezione dei dati personali è costituito dalla Direttiva n. 95/46/CE del Parlamento Europeo e del Consiglio recante "*tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*". Trattasi di uno strumento normativo che riveste la particolarità di avere incorporato numerosi dei principi di cui alla Convenzione n. 108 del Consiglio d'Europa, oltre che di aver codificato quelli affermati dalla giurisprudenza della Corte di Strasburgo e della Corte di Giustizia. Invero, come riconosciuto dal suo stesso considerando n. 11, la Direttiva "*precisa ed amplia i contenuti enunciati dalla Convenzione 108 sul trattamento automatizzato dei dati*".

Attraverso l'adozione di un unico strumento normativo a carattere generale, destinato a dettare una disciplina uniforme per regolamentare pressoché tutte le tipologie di trattamento dei dati personali, il diritto europeo si distingue, così, nettamente rispetto all'approccio settoriale tipico del

diritto statunitense, caratterizzato da una moltitudine di leggi e regolamenti che disciplinano ciascun singolo aspetto del trattamento dei dati personali.

Ciò premesso, come implicitamente affermato dalla Corte di Giustizia nella causa *Osterreicher Rundfunk*, obiettivo della Direttiva 95/46 non è soltanto quello di garantire la libera circolazione dei dati personali ma, anche quello di assicurare la salvaguardia dei diritti fondamentali della persona e di offrire ai dati personali un grado di tutela elevato ed equivalente all'interno di tutti gli Stati membri[292].

La Direttiva 95/46/CE, inoltre, mira a garantire un elevato standard di protezione dei dati non soltanto in funzione della loro circolazione infra-comunitaria, ma anche nell'ipotesi di loro trasferimento verso Paesi terzi. In quest'ottica, infatti, la Direttiva 95/467/CE del 24.10.1995 contiene una nutrita serie di disposizioni che disciplinano il trasferimento dei dati personali all'estero.

Invero, il capo IV della medesima, agli artt. 25 e ss., predispone un regime speciale implicante norme specifiche, teso a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso paesi terzi. Tale capo istituisce un regime complementare rispetto al regime generale attuato dal capo II della suddetta direttiva, riguardante la liceità di trattamenti di dati personali.

In questo campo la direttiva delinea un meccanismo di dialogo istituzionale tra Stati membri e Commissione, in virtù del quale essi si informano reciprocamente nei casi in cui il livello di protezione offerto dagli Stati terzi venga giudicato non affidabile. Dalla ripartizione di competenze così concepita discende un parallelismo provvisorio anche nella spettanza dei poteri di negoziazione con Stati terzi. Gli Stati saranno legittimati a concludere autonomamente accordi in materia, sino a che non siano poste in essere convenzioni tra l'Unione europea e i medesimi soggetti terzi. La Commissione può in effetti avviare, "al momento opportuno", negoziati per porre rimedio alla situazione risultante da sue decisioni sull'assenza di norme di salvaguardia sufficienti, in fatto di tutela dei dati personali, in certi Paesi. A questo proposito è stato osservato come a decidere dell'"opportunità" del momento in cui avviare i negoziati sarà, evidentemente, la Commissione stessa e che l'espressione del "momento opportuno" sembra, altresì, escludere la possibilità da parte di altre Istituzioni comunitarie o degli Stati membri di contestare l'avvio di determinati negoziati o, al contrario, di esperire un ricorso in carenza contro l'inerzia della Commissione[293].

Un'altra leva cui è possibile ricorrere per ovviare ad insufficienti garanzie per i titolari dei dati residenti nella UE sarà quella di impegni autonomi negoziati con determinati responsabili del

[292] Cfr. par. 39 della Sentenza della Corte (Quarta Sezione) del 18 ottobre 2007 nelle Cause riunite C-465/00, C-138/01 e C-139/01 Österreichischer Rundfunk

[293] Paolo Pallaro, cit. sub nota 1

trattamento, che assicurino l'apprestamento in proprio di "garanzie sufficienti per la tutela della vita privata e dei diritti e delle libertà fondamentali delle persone" in merito ad un corretto trattamento dei loro dati. In pratica si tratterà di responsabili fortemente "internazionalizzati" nella loro struttura ed economicamente importanti, solidi e forti, quali multinazionali, grosse società (si pensi al settore assicurativo-finanziario, delle telecomunicazioni, o delle compagnie aeree), enti transnazionali, o loro associazioni di categoria.

Ciò premesso, l'obiettivo del capo IV viene definito nei considerando 56-60 della direttiva 95/46, i quali dispongono in particolare che, se la tutela delle persone garantita dalla direttiva non osta al trasferimento di dati personali verso paesi terzi che prevedano un livello di protezione adeguato, l'adeguatezza deve essere valutata in funzione di tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti. Quando un paese terzo non offre un livello di protezione adeguato, il trasferimento di dati personali verso tale paese dev'essere vietato.

Invero, in un'epoca caratterizzata dalla globalizzazione e dalla tecnologia informatica, un provvedimento normativo che si limitasse a disciplinare i movimenti di dati personali esclusivamente all'interno del territorio europeo sarebbe, oltre che anacronistico, anche facilmente aggirabile. Sarebbe, ad esempio, sufficiente per una società operante in Europa costituire una filiale in un paese terzo, ove la legislazione a tutela dei dati personali sia meno severa, o addirittura inesistente, al fine di ivi trasferirvi tutti i dati personali da sottoporre a trattamento ed eludere, così, le garanzie previste dalla normativa europea in materia di *data protection*.

A tale circostanza soccorre, tuttavia, l'art. 25 della direttiva 95/46 il quale impone agli Stati membri ed alla Commissione vari obblighi di controllo sui trasferimenti di dati personali verso i paesi terzi, tenuto conto del livello di protezione concesso a siffatti dati in ciascuno di tali paesi.

In particolare, l'art. 25, n. 4, della direttiva 95/46 prevede che, qualora la Commissione constati che un paese terzo non garantisca un livello di protezione adeguato, gli Stati membri adottano le misure necessarie per impedire ogni trasferimento di dati personali verso il paese terzo in questione.

In altre parole il livello adeguato di protezione offerto dal Paese terzo in questione rappresenta il criterio ispiratore di tutta la disciplina in materia di trasferimento all'estero di dati personali. La regola di consentire il trasferimento soltanto in presenza di un livello adeguato di protezione subisce poi le eccezioni che vengono tassativamente indicate dal successivo art. 26.

Fermo restando quanto finora esposto, si deve evidenziare, anzitutto, come dalla norma risulti evidente che il legislatore comunitario ha inteso disciplinare i flussi transfrontalieri dei dati solo quando sono diretti verso Paesi terzi , vale a dire verso Paesi non facenti parte dell'Unione Europea. In uno spazio nel quale non vi sono più frontiere, parlare di flussi transfrontalieri in relazione agli spostamenti di dati personali tra Paesi membri non ha molto senso e risulta oltremodo

contraddittorio se rapportato all'intenzione del legislatore comunitario, che era quella di creare uno spazio giuridico omogeneo, nel quale vi fosse un livello di tutela equivalente tra i Paesi membri in materia di protezione delle persone rispetto al trattamento dei loro dati personali[294].

In secondo luogo, si deve osservare come la direttiva utilizzi il concetto di *"livello adeguato di protezione*" senza però definirlo, lasciando così un evidente margine di apprezzamento alla Commissione ed agli Stati membri nel valutare il contenuto delle garanzie offerte dalla legislazione del paese terzo a tutela dei dati personali.

In ogni caso, il secondo paragrafo dell'art. 25 contiene la precisazione secondo la quale, "*l'adeguatezza del livello di protezione garantito da un Paese terzo è valutata con riguardo a tutte le circostanze relative ad un trasferimento o ad una categoria di trasferimenti di dati*". in particolare, secondo la disposizione testé richiamata, sono presi in considerazione "*la natura dei dati, le finalità del o dei trattamenti previsti, il Paese d'origine e il Paese di destinazione finale, le norme di diritto, generali o settoriali, vigenti nel Paese terzo di cui trattasi, nonché le regole professionali e le misure di sicurezza ivi osservate".*

Il testo delle disposizione citata chiarisce, dunque, che l'adeguatezza del livello di protezione offerto dalla legislazione del paese terzo destinatario del flusso di dati deve, innanzitutto, essere valutata in funzione della natura dei dati, nonché della finalità del o dei trattamenti previsti, avuto altresì riguardo al Paese d'origine e a quello di destinazione finale. Si tratta di una formulazione diretta, con tutta evidenza, non già ad attribuire una definizione, bensì a fornire una chiave interpretativa, suscettibile di orientare l'applicazione pratica della norma. In tal senso la disposizione suggerisce, ad esempio, l'esigenza di valutare con maggiore attenzione e scrupolo il livello di adeguatezza della protezione offerta dal Paese terzo in questione laddove oggetto del trasferimento siano dati cd. "sensibili".

Inoltre, la disposizione in esame precisa che oggetto di valutazione non è soltanto la legge dello Stato terzo, bensì anche "l*e regole professionali e le misure di sicurezza ivi osservate*". Pertanto,nell'ottica della direttiva europea, oggetto di valutazione non saranno soltanto le fonti di rango legislativo, ma potranno essere prese in considerazione anche fonti di rango sub-legislativo di carattere regolamentare e finanche deontologico. Una tale impostazione riflette la consapevolezza, da parte dell'ordinamento giuridico europeo, che al di fuori dei confini del Vecchio Continente, la protezione dei dati personali può anche non necessariamente essere soggetta al presidio della legge ordinaria.

[294] Giannaccari Andrea "Brevi note in tema di clausole contrattuali tipo per i trasferimenti di dati personali verso i paesi terzi" Danno e Resp. 2001, 10, 910

Ciò premesso, la nozione di livello adeguato di protezione, stante la sua genericità, ha formato oggetto di un articolato parere da parte del Gruppo di lavoro ex art. 29, pubblicato nel 1997[295], nell'intento di "*ridurre il campo semantico di una clausola che, in ogni caso, conserva per propria natura un certo spazio ermeneutico disponibile sia per le decisioni procedurali delle Istituzioni comunitarie nelle relazioni con i Paesi terzi, sia per gli organi competenti a risolvere eventuali controversie, in dipendenza dalle circostanze caratterizzanti i singoli casi*[296]".

Infatti, tenuto conto che il regime delle deroghe previsto dal successivo art. 26 si caratterizza per essere formulato in maniera tassativa, numerosi sono i casi di trasferimento di dati personali verso paesi terzi suscettibili di non essere ricompresi nel suddetto elenco, rendendo così indispensabile un sindacato in punto di adeguatezza ai sensi del primo paragrafo dell'art. 25 della direttiva. Da qui la necessità di elaborare dei parametri di valutazione generali al fine di guidare gli operatori nella valutazione dell'adeguatezza degli standard di protezione offerti dalla normativa dei Paesi terzi in materia di *data protection*.

Come è stato osservato dal Gruppo di Lavoro in tale sede, dato il numero enorme di trasferimenti di dati personali che avvengono su scala giornaliera nessuno Stato membro, a prescindere dalle specifiche modalità di trasposizione dell'art. 25 della Direttiva nel proprio diritto interno, sarebbe in grado di esaminare ciascun singolo caso di trasferimento in dettaglio. Diviene, pertanto, necessario elaborare dei criteri generali o comunque dei meccanismi suscettibili di razionalizzare il processo decisionale con riguardo ad un grande numero di casi[297].

Nel suo parere il Gruppo di Lavoro ha avuto modo di constatare come, a livello Europeo, la tendenza generale degli Stati sia stata, storicamente, quella di incorporare la disciplina della protezione dei dati personali nelle proprie leggi interne. Tale tendenza ha permesso la possibilità di sanzionarne l'inosservanza e di concedere agli individui dei mezzi di ricorso interni. Inoltre, molti Stati membri, oltre ad essere destinatari della Direttiva 95/46, risultava essere altresì parte alla Convenzione 108 del Consiglio d'Europa sul Trattamento automatizzato di dati ed hanno altresì provveduto ad implementare le linee guida del OCSE del 1980 e quelle delle Nazioni Unite del 1990.

Pertanto, secondo il parere del Gruppo di Lavoro, incrociando le disposizioni della direttiva con quelle degli altri strumenti internazionali citati sarebbe stato possibile pervenire ad un nucleo duro di principi in materia di protezione dei dati e dei meccanismi volti ad assicurarne il rispetto, tale da

[295] Cfr. Art. 29 Working Party, "*Discussion Document: First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy*", reperibile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1997/wp4_en.pdf aggiornato al 2 ottobre 2012

[296] Paolo Pallaro, nota 281

[297] Cfr. Art. 29 Working Party cit. sub nota 3

poter esser considerati come un requisito minimo affinché il livello di protezione offerto potesse considerarsi adeguato.

Sulla scorta di tali considerazioni il Gruppo di Lavoro ha enucleato alcuni principi, il cui rispetto potrebbe essere considerato come un requisito minimo affinché la protezione possa ritenersi adeguata. Ovviamente, non si tratta di un elenco tassativo, poiché in alcuni casi particolari potrebbe sorgere la necessità di aggiungere ulteriori elementi di valutazione, laddove in altri casi potrebbe risultare necessario ridurre la lista dei requisiti. E' infatti il grado di rischio che il trasferimento di dati comporta a costituire il fattore determinante i precisi requisiti di un particolare caso.

Ciò premesso, tra i principi minimi il Gruppo di Lavoro individua anzitutto, il principio della limitazione della finalità del trattamento, secondo cui i dati dovrebbero essere trattati per una finalità specifica e, conseguentemente utilizzati o inoltrati per scopi non incompatibili con quello del trasferimento.

In secondo luogo, viene individuato il principio della qualità dei dati e di proporzionalità, in virtù del quale i dati dovrebbero essere accurati e aggiornati, oltre che pertinenti e quantitativamente non esorbitanti rispetto allo scopo per il quale vengono trasferiti.

In terzo luogo, il principio di trasparenza impone che gli individui vengano informati delle finalità del trattamento, e dell'identità del responsabile del trattamento nel paese terzo. Allo stesso modo il principio di sicurezza esige che vengano adottate delle misure tecniche ed organizzative volte a tutelare i dati raccolti dai rischi del trattamento.

Viene poi previsto il diritto di accesso, rettifica e opposizione, a mente del quale il titolare dei dati dovrebbe avere diritto ad ottenere una copia di tutti i dati che lo riguardano e che vengono sottoposti a trattamento, e il diritto a rettificare i dati che si dimostrino inaccurati. Inoltre, in alcuni casi, dovrebbe avere diritto ad opporsi al trattamento dei suoi dati.

Infine, viene previsto il principio del divieto di ulteriore trasferimento, la cui finalità è quella di evitare che i dati vengano successivamente trasferiti verso Paesi che non offrono un adeguato standard di protezione al fine di aggirare le tutele previste dalla normativa. Specularmente, dunque, i trasferimenti ulteriori verranno consentiti soltanto laddove il paese terzo offra a sua volta un adeguato livello di protezione.

Ciò premesso, il Gruppo di lavoro ha notato come, sebbene in Europa vi sia un generale consenso tra gli Stati circa il fatto che i principi a tutela dei dati personali debbano essere previsti e tutelati dalla legge e che vi è necessità di un sistema di supervisione esterna da parte di un'autorità indipendente, questi principi possono non essere condivisi altrove nel mondo.

Sulla base di tali considerazioni il Gruppo i Lavoro, nel suo parere sull'applicazione degli articoli 25 e 26 della Direttiva sulla protezione dei dati[298], ha individuato le seguenti priorità affinché il sistema procedurale di protezione dei dati utilizzato da un paese terzo possa ritenersi offrire una protezione adeguata.

Innanzitutto il sistema procedurale deve, in linea generale, comportare un buon livello di rispetto delle regole. Secondo il parere espresso dal Gruppo di Lavoro un buon sistema di tutela è, infatti, generalmente caratterizzato da un'elevata consapevolezza, da parte dei responsabili del trattamento, dei loro obblighi e, sul versante dei titolare dei dati, dei rispettivi diritti e delle modalità di loro esercizio. L'esistenza di sanzioni efficaci e dissuasive può giocare un importante ruolo nell'assicurare il rispetto delle regole. Inoltre, un buon sistema procedurale di protezione dovrebbe fornire supporto ed aiuto ai singoli titolari di dati nell'esercizio dei loro diritti. L'individuo dovrebbe essere, cioè, in grado di ottenere il rispetto dei suoi diritti in maniera rapida ed efficace e senza costi proibitivi. Infine il sistema procedurale di protezione dovrebbe, nell'ottica del Gruppo di Lavoro, fornire appropriata riparazione alla parte lesa, le quali dovrebbero includere compensazioni e sanzioni in caso di mancato rispetto delle norme.

Una volta individuato il contenuto dei principi e dei meccanismi procedurali necessari affinché la protezione offerta da un paese terzo possa considerarsi adeguata il Gruppo di Lavoro si è chiesto se i paesi che hanno ratificato la Convenzione 108 possano considerarsi come offrenti un livello di protezione adeguato.

In quest'ottica è stato notato che, seppur la Convenzione 108 richieda agli Stati parte di ratificarne il contenuto con legge, essa non detta alcuna disposizione con riguardo ai meccanismi sanzionatori e di controllo volti ad assicurare il rispetto delle medesime. Ciò seppure gli Stati che hanno ratificato la Convenzione hanno in genere aggiunto siffatti meccanismi.

Allo stesso modo, come si è osservato nel capitolo dedicato, la Convenzione 108 non vieta i trasferimenti ulteriori di dati personali verso paesi che non sono parte alla medesima. Ciò determina il rischio che un paese parte alla Convenzione possa essere usato come piattaforma per il trasferimento di dati dall'Unione Europea verso un ulteriore paese terzo con un livello di protezione interamente inadeguato. Infine, la Convenzione 108 nulla prevede in tema di pubblicità commerciale o di decisioni individuali automatizzate.

In altre parole, secondo il Gruppo di Lavoro , il trasferimento di dati personali verso un paese che ha ratificato la Convenzione 108 del Consiglio d'Europa sarà assentibile a condizione che la legge di ratifica interna preveda dei meccanismi sanzionatori e di controllo e che il paese in

[298] Cfr. Working Party on the Protection of Individuals with regard to the Processing of Personal Data: "Working Document: Transfer of personal data to third countries:applying articles 25 and 26 of the EU data protection directive" reperibile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_en.pdf aggiornato al 2.10.2012

questione sia il destinatario finale del flusso di dati e non un paese intermediario all'interno del quale i dati si limitano a transitare.

Successivamente, il Gruppo di lavoro ha tentato di formulare dei criteri generali per valutare il livello di protezione offerto da quei Paesi terzi in cui la tutela dei dati non viene assicurata da fonti di rango legislativo bensì da un sistema di *self regulation.* Data la rilevanza della questione delle considerazioni maggiormente analitiche verranno sviluppate nei paragrafi successivi. In questa sede

Sulla scorta delle osservazioni che precedono, dunque, il Gruppo di Lavoro ha ravvisato la necessità di elaborare una sorta di "lista bianca" di paesi terzi, i quali possono essere considerati come offrenti un livello adeguato di protezione. Tale lista, sempre secondo il Gruppo di Lavoro, dovrebbe avere carattere meramente orientativo, lasciando impregiudicata la valutazione relativa a casi specifici che presentano problematiche particolari[299].

In quest'ottica, come si è visto, lo sviluppo di una "lista bianca" di paesi offrenti un livello adeguato di protezione presenta diverse difficoltà. Infatti, molti paesi terzi non prevedono, ad esempio, a livello legislativo una protezione uniforme in tutti i settori economici, come negli Stati Uniti, ove esiste una legge sulla protezione dei dati a livello pubblico ma non a livello privato. Allo stesso modo, problemi possono sorgere con riguardo a quei paesi che hanno un'articolazione federale, ove sussistono spesso delle differenze tra i vari stati che costituiscono la federazione. Infine, svariati problemi possono insorgere con riferimento ai paesi in cui la protezione dei dati viene delegata alla self-regulation.

3. Le decisioni sull'adeguatezza della Commissione

La Direttiva offre gli strumenti necessari all'elaborazione di una siffatta lista bianca. Infatti, la Direttiva contempla, in tale ottica, un meccanismo di cooperazione tra Stati membri e Commissione Europea in virtù del quale comunicano a vicenda tutti i casi in cui ritengano che un Paese terzo non offra un livello adeguato di protezione (art. 25 par. 3).

Alla Commissione poi viene attribuito un potere decisionale che si fonda sul meccanismo stabilito dall'art. 31 della Direttiva il quale prevede, sostanzialmente, che essa venga affiancato da un Comitato di gestione e si avvalga, altresì della collaborazione fornitale (art. 29, par. 1) dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali (Gruppo ex art. 29), composto dai rappresentanti delle autorità di controllo nazionale incaricate di sorvegliare, nel

[299] Cfr. Art. 29 Working Party cit. sub nota 3

territorio dello Stato Membro, l'applicazione delle disposizioni di attuazione della Direttiva[300]. A tali autorità nazionali di controllo spetta la designazione del membro che le rappresenta nel Gruppo, ai cui lavori partecipa, senza diritto di voto, la stessa Commissione. Il Gruppo si avvale inoltre della presenza attiva (con diritto di voto, cioè) del Supervisore europeo per la protezione dei dati[301].

Indottrina è stato sottolineato come il ruolo del Gruppo, malgrado i pareri da esso forniti rivestano carattere consultivo, non tolleri fraintendimenti[302]: è composto infatti di soggetti che esercitano, Stato per Stato, una autorità indipendente di controllo sull'applicazione della normativa nazionale (come armonizzata dalla Direttiva) godendo di poteri investigativi, di intervento, di promozione di azioni giudiziarie in caso di violazione di norme nazionali. Di conseguenza esso si trova «*in una posizione di osservatorio privilegiato di tutte le pertinenti normative, europee e nazionali*»; di più, il Gruppo ex art. 29 viene maturando un'esperienza «*su scala internazionale circa leggi, prassi e problemi inerenti alla protezione dell'autodeterminazione informativa*»[303]. Le indicazioni contenute nei suoi pareri assumono anzi, alla luce della natura fondamentale del diritto da proteggere, «un valore aggiunto rispetto al disposto della direttiva», incidendo sulla corretta interpretazione da dare a tale disposto[304].

La procedura alla quale la disposizione in questione faceva riferimento era quella di gestione cui all'artt. 4 della Decisione 1999/468/CE[305] (comitatologia), successivamente abrogata dal Regolamento n. 182/2011[306].

Tale procedura prevedeva l'intervento di un comitato di rappresentanti degli Stati membri presieduto da un rappresentante della Commissione. La Commissione sottoponeva le misure da prendere al comitato che emanava un parere nel termine di tre mesi del quale la Commissione

[300] Art. 28, par. 1. Si tratta di autorità indipendenti nell'esercizio delle funzioni loro attribuite, autorità che dispongono (art. 28, par. 3) di poteri investigativi (diritto di accesso ai dati oggetto di trattamento e di raccolta di ogni informazione necessaria all'adempimento della funzione), di poteri effettivi d'intervento (tra cui, oltre alla formulazione dei pareri ex art. 20, quello di ordinare congelamento, cancellazione o distruzione dei dati, oppure di vietare un trattamento, di rivolgere un avvertimento al responsabile del trattamento, nonché di adire le istituzioni politiche nazionali, in primis il Parlamento) e di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali. Sull'Istituto del Garante per la privacy nell'ordinamento interno italiano v. A. SIMONCINI, Autorità indipendenti e «costruzione» dell'ordinamento giuridico: il caso del Garante per la protezione dei dati personali, in Dir. pubbl., 1999, p. 851 ss

[301] Istituito - ex art. 286, par. 2 del Trattato CE - dal Reg. 45/2001 del PE e del Consiglio del 18 dicembre 2000 sulla protezione degli individui con riguardo al trattamento dei dati personali da parte delle istituzioni della Comunità e sulla libera circolazione di tali dati, in G.U. L 8 del 12 gennaio 2001. L'art. 46, lett. f) e g) del Reg. 45/2001 stabilisce in capo al Supervisore l'obbligo di cooperare con il Gruppo ex art. 29

[302] Lauso Zagato, nota 285

[303] P. Pallaro, "*Libertà della persona e trattamento dei dati personali nell'Unione europea*", Milano, 2002, p. 47

[304] Idem

[305] Dec. 28-6-1999 n. 1999/468/CE del Consiglio recante modalità per l'esercizio delle competenze di esecuzione conferite alla Commissione. Pubblicata nella G.U.C.E. 17 luglio 1999, n. L 184

[306] Reg. (CE) 16-2-2011 n. 182/2011 del Parlamento Europeo e del Consiglio che stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione. Pubblicato nella G.U.U.E. 28 febbraio 2011, n. L 55.

teneva la massima considerazione, pur conservando tuttavia un ampio margine di apprezzamento nell'esecuzione. La Commissione adottava misure immediatamente applicabili. Tuttavia, se tali misure non erano conformi al parere del comitato, la Commissione le comunicava immediatamente al Consiglio. In quest'ultimo caso, la Commissione poteva differire l'applicazione delle misure da essa decise mentre Il Consiglio, deliberando a maggioranza qualificata, può prendere una decisione diversa entro il termine di tre mesi.

La dottrina ha sempre evidenziato come il risultato delle procedure di cui alla decisione Comitatologia fosse comunque quello di riattribuire sostanzialmente la competenza di esecuzione al Consiglio stesso: *"si ha una sorta di delega condizionata, con ritorno eventuale al Consiglio, vanificando in gran parte l'impegno a delegare voluto dal Trattato"* [307]. Come si accennava poc'anzi, oggi la decisione 1999/468/CE è stata abrogata dal Regolamento n. 182/2011 con il quale si è provveduto a ordinare e semplificare la procedura dei comitati alla luce del Trattato di Lisbona.

Con il nuovo regolamento viene mantenuta la struttura dei comitati, riorganizzati e razionalizzati per affinità, i cui lavori sono periodicamente comunicati al Parlamento e al Consiglio e devono essere accessibili al pubblico. Inoltre, la procedura consultiva diviene, salvo le eccezioni previste nel regolamento stesso, la regola generale per cui la Commissione decide le misure da adottare limitandosi a tenere in massima considerazione il parere formulato dal comitato,

Ciò premesso, la potestà decisionale della Commissione può sfociare tanto nella constatazione che un Paese Terzo non offra un livello adeguato di protezione dei dati, con conseguente obbligo ex art. 25 par. 4 della Direttiva per gli Stati membri di adottare le misure necessarie per impedire ogni trasferimento di dati della stessa natura verso il Paese terzo in questione, quanto nella constatazione che un Paese terzo garantisce un livello di protezione adeguato, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali.

La conseguenza di una decisione di adeguatezza è che, in tal caso, gli Stati membri possono trasferire dati personali nel paese terzo in questione senza richiedere ulteriori garanzie. E' opportuno rilevare che le decisioni di adeguatezza vengono adottate anche sulla scorta del parere espresso dal Gruppo di Lavoro ex art. 29 sull'applicabilità degli artt. 25 e 26 della Direttiva[308].

Inoltre, Data la diversità degli approcci alla protezione dei dati nei paesi terzi, è opportuno che la valutazione dell'adeguatezza avvenisse e che ogni decisione, basata sull'articolo 25, §6, della direttiva 95/46/CE, fosse presa ed attuata senza da luogo a discriminazioni arbitrarie o ingiustificate

[307] G. Strozzi, nota 142

[308] Trasferimenti di dati personali verso paesi terzi: applicazione degli articoli 25 e 26 della direttiva comunitaria sulla tutela dei dati, documento adottato dal gruppo di lavoro il 24 luglio 1998, disponibile al seguente indirizzo: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wpdocs_98.htm

verso o tra paesi terzi in cui esistono condizioni analoghe e senza dar luogo a barriere occulte per gli scambi commerciali, visti gli attuali impegni della Comunità a livello internazionale

Proprio con riferimento agli impegni internazionali, la Direttiva dà mandato alla Commissione di avviare, al momento opportuno, negoziati per porre rimedio alla situazione risultante dalla constatazione negativa (art. 25 par. 5).

Come verrà illustrato nel paragrafo successivo la Commissione ha emanato diverse decisioni con riguardo all'adeguatezza del livello di protezione offerto dalle legislazioni di alcuni stati terzi con riguardo alla protezione dei dati personali, segnatamente nei confronti di: Argentina, Canada, Svizzera, Stati Uniti, ed inoltre Isola di Man e Isole del Canale (Bailato di Guernsey). Ancor prima dell'adozione di tali decisioni "positive" il "Gruppo di lavoro ex art. 29" aveva raccomandato di "*constatare che l'Ungheria assicura un livello di protezione adeguato ai sensi dell'art. 25 paragrafo 6*" della direttiva comunitaria, essendo dotata di una legge del 1992 sulla tutela dei dati personali, di una protezione costituzionale del diritto al rispetto della vita privata e delle informazioni personali, nonché di numerose norme specifiche in materia di direct-mailing, ricerca scientifica, statistica, trattamenti dei dati sanitari[309]

Tralasciando per il momento il rapporto con gli USA, negli altri casi significativi indicati ci si trova in presenza di normative introdotte negli ordinamenti federali rispettivamente di Argentina, Canada e Svizzera, a coronamento dello sforzo compiuto dai legislatori di tali Stati per consentire che tali ordinamenti siano giudicati idonei a fornire una protezione adeguata alla stregua dei parametri UE[310]. In tutti e tre i casi la Commissione, seguendo il parere del Gruppo ex art. 29, verifica la sostanziale corrispondenza del livello di tutela della privacy garantito dalla nuova legge con quello in vigore nella UE. Unico punto di preoccupazione è il fatto che, trattandosi di Stati federali, la nuova legge possa non trovare applicazione a livello locale.

Con decisione 20-12-2001 n. 2002/2/CE[311], innanzitutto, la Commissione ha sancito l'adeguatezza della protezione fornita dalla legge canadese, per effetto del "*Canadian Personal Information Protection and Electronic Documents Act"*[312], sulla tutela delle informazioni personali e sui documenti elettronici. In particolare La legge canadese sulla tutela delle informazioni personali e sui documenti elettronici («the Canadian Act») del 13 aprile 2000 si applica dal 1° gennaio 2001 alle informazioni personali rilevate o comunicate da organizzazioni quali imprese, stabilimenti o aziende operanti a livello federale[313]. Solo dal 2004 il PIPED Act viene applicato a

[309]Cfr. l'Opinione n. 6/99 del 7 settembre 1999 (WP24)
[310] Lauso Zagato, nota 285
[311] Pubblicata nella G.U.C.E. 4 gennaio 2002, n. L 2
[312]Testo reperibile su http://www.parl.gc.ca/36/2/parlbus/chambus/house/bills/government/C-6/C-6_4/C-6_cover-E.html
[313] Con esclusione dei dati sanitari personali; per questi ultimi la legge si applica a partire dal 1° gennaio 2002.

qualsiasi organizzazione, federale o meno, che utilizzi nel territorio canadese dati personali nell'ambito di attività commerciali[314]. L'art. 26, par. 2 della legge canadese prevede che, ove le province si dotino di normative giudicate dai competenti organi centrali «adeguate» alla stregua della legge federale, alla trasmissione di dati relativa a transazioni interne alla provincia sia applicata tale normativa. Il PIPED Act continuerà invece ad applicarsi alle attività di rilevazione, utilizzo e comunicazione dei dati fra province, nonché nei casi non coperti dalla legislazione provinciale[315].

Successivamente, con decisione 30-6-2003 n. 2003/490/CE[316] la Commissione ha dichiarato l'adeguatezza della tutela dei dati personali fornita in Argentina, sulla quale si è espresso anche il Gruppo di Lavoro ex art. 29[317]. Per quanto riguarda l'Argentina, le norme giuridiche relative alla tutela dei dati personali sono state inserite in norme a carattere generale e in norme settoriali, tutte giuridicamente vincolanti.

In particolare l'art. 43, par. 3 della Costituzione del 1994 prevede un ricorso giurisdizionale chiamato *habeas data*[318]. La decisione di adeguatezza della Commissione CE, non diversamente dal precedente parere favorevole espresso dal Gruppo ex art. 29, si fonda sul lavoro di consulenza svolto a stretto contatto con le autorità argentine incaricate di promulgare la normativa applicativa della disposizione costituzionale[319]. Il giudizio positivo sulla legislazione emanata a livello centrale si accompagna anche in questo caso a preoccupazioni relative all'applicazione della stessa a livello provinciale.

Nel caso della Svizzera, la Decisione della Commissione che definiva adeguato il livello di protezione offerto dal Swiss Federal Act on Data Protection (SFADP) è stata presa malgrado le preoccupazioni espresse dal Gruppo ex art. 29 circa l'adeguatezza della legislazione cantonale. Il Gruppo richiama quanto già affermato nel citato WP 12: per quanto l'adesione della Svizzera alla Convenzione n. 108 sia importante, il conseguimento degli obiettivi di questa non è tale da garantire automaticamente l'esistenza di un livello sufficiente di tutela ai fini dell'applicazione della Direttiva

[314] Ciò ad esclusione delle organizzazioni governative soggette al Federal Privacy Act, a quelle regolate dal settore pubblico a carattere provinciale, alle organizzazioni senza scopo di lucro; il PIPED Act non si applica neppure a quei dati sui lavoratori dipendenti che siano usati per scopi non commerciali

[315] Nel marzo 2002 la Commissione CE ha emanato delle Frequently Asked Questions (FAQ) «on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents» per agevolare i privati che debbano conformarsi alle norme del PIPED Act.

[316] Pubblicata nella G.U.U.E. 5 luglio 2003, n. L 168

[317] Parere 4/2002 sul livello di protezione dei dati personali in Argentina - WP 63 del 3 ottobre 2002 disponibile al seguente indirizzo:http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm

[318] Si tratta di un'azione concessa a chiunque per «venire a conoscenza di tutti i dati che lo riguardano presenti presso registri o banche dati pubblici oppure banche dati private aventi finalità informative». Alla norma è stata riconosciuta dalla giurisprudenza la diretta applicabilità. Il principio di habeas data costituzionale si sta peraltro affermando nei principali ordinamenti giuridici sudamericani

[319] Legge 25.326 sulla tutela dei dati personali del 4 ottobre 2000 (consultabile al sito www.protecciondedatos.com.arg) e Regolamento approvato con decreto 1558/2001 del 3 dicembre 2001

95/46. Ciò a causa di alcuni limiti, tra i quali: mancanza di restrizioni al trasferimento dei dati verso Stati terzi non parte alla Convenzione; mancanza di obbligo per i responsabili del trattamento di fornire informazioni all'interessato prima del trattamento; assenza di previsioni in materia di pubblicità commerciale e di decisioni individuali automatizzate; mancata previsione di istanze ad hoc per svolgere indagini indipendenti e risolvere controversie Essendosi negli anni successivi avuto, dietro pressione degli organi comunitari, l'inserimento di clausole sulla tutela dei dati nelle Costituzioni di 16 su 26 cantoni (ma alcune altre sono in corso), il Documento di lavoro dei servizi della Commissione dell'autunno 2004 (41) prende atto con soddisfazione di tale positiva evoluzione.

Ancora, con decisione 8-5-2008 n. 2008/393/CE[320] la Commissione ha affermato l'adeguata protezione dei dati personali da parte del Bailato di Jersey[321]. Analoga decisione è stata presa con riguardo alle Isole Faer Oer[322] con provvedimento del 5-3-2010 n. 2010/146/UE[323] sulla scorta del parere del Gruppo di Lavoro ex art. 29[324]. Il Principato di Andorra[325] (Dec.19-10-2010 n. 2010/625/UE[326]) . la Commissione ha dichiarato l'adeguatezza del livello di protezione offerto dalle leggi dello Stato di Israele[327] e della Repubblica Orientale di Uruguay[328].

4. Il regime delle deroghe al livello adeguato di protezione

Come si è detto profusamente nelle pagine precedenti, il trasferimento all'estero di dati personali è consentito soltanto laddove il Paese terzo offra un livello adeguato di protezione. Tuttavia, come per ogni regola, esistono delle eccezioni.

Il regime delle eccezioni è codificato all'art. 26 della Direttiva 95/46/CE, il quale disciplina una serie di circostanze in cui il trasferimento dei dati personali verso un Paese terzo che non assicura

[320] Pubblicata nella G.U.U.E. 28 maggio 2008, n. L 138

[321] Il Baliato di Jersey è una dipendenza della Corona britannica (senza essere una zona del Regno Unito né una colonia) ma completamente indipendente, tranne che per le relazioni internazionali e la difesa, di competenza del governo britannico; il Baliato di Jersey va dunque considerato un paese terzo ai fini della direttiva 95/46/CE

[322] Le Isole Faer Øer sono una regione autonoma del Regno di Danimarca. Quando la Danimarca è entrata a far parte della Comunità europea, nel 1973, le Isole Faer Øer non vi hanno aderito. Vanno quindi considerate un paese terzo ai fini della direttiva 95/46/CE

[323] Pubblicata nella G.U.U.E. 9 marzo 2010, n. L 58

[324] Parere 9/2007 sul livello di protezione dei dati personali nelle Isole Faer Øer, adottato il 9 ottobre 2007, disponibile sul sito http://ec. europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp142_it.pdf

[325] Andorra è uno Stato dotato di un sistema di coprincipato parlamentare, in cui le funzioni dei coprincipi sono esercitate dal presidente della Repubblica francese e dall'arcivescovo di Urgell

[326] Pubblicata nella G.U.U.E. 21 ottobre 2010, n. L 277

[327] Dec. 31-1-2011 n. 2011/61/UE Pubblicata nella G.U.U.E. 1 febbraio 2011, n. L 27.

[328] Dec. 21-8-2012 n. 2012/484/UE Pubblicata nella G.U.U.E. 23 agosto 2012, n. L 227.

un livello adeguato di protezione viene eccezionalmente consentito. Come si vedrà si tratta di un elenco di ipotesi tassative, per la maggior parte, i rischi per il titolare dei dati sono relativamente bassi ovvero gli interessi del medesimo obliterano qualsiasi preoccupazione in merito alla protezione dei dati.

Si tratta di una norma di carattere eccezionale poiché il responsabile del trattamento, nelle ipotesi ivi previste, non soltanto non è tenuto a preoccuparsi se il livello di protezione dei dati nel Paese terzo sia o meno adeguato, ma non deve neppure richiedere alcun tipo di autorizzazione preventiva al trasferimento da parte delle autorità competenti. Allo stesso modo, queste disposizioni non richiedono che il destinatario del flusso dei dati rispetti i requisiti della direttiva con riguardo al trattamento dei dati nel proprio Paese (es. principio di sicurezza, diritto di accesso ecc.). In ogni caso, giova ribadire come, anche in presenza di queste ipotesi di carattere eccezionale, le deroghe previste dall'art. 26 non possono applicarsi disgiuntamente rispetto alle altre disposizioni della direttiva. Come esplicitamente affermato dall'art. 25, infatti, queste disposizioni si applicano "senza pregiudizio per il rispetto delle disposizioni nazionali adottate ai sensi delle altre disposizioni di questa direttiva". Ciò significa che, al di là delle disposizioni su cui ci si basa ai fini del trasferimento di dati verso un paese terzo, altre disposizioni della direttiva devono essere rispettate. Nello specifico dunque, ciò significa che qi sensi del paragrafo 60 del preambolo della direttivam che laddove dati sensibili siano implicati nel trasferimento, i requisiti dell'art, 8 della Direttiva dovrebbero essere soddisfatti. Ciò puà implicare che uno specifico trasferimento può bassarsi sull'art 26 ove applicabile soltanto se le condizioni di cui all'art. 8 sono state rispettate.

Ai sensi dell'art. 26, il trasferimento di dati personali verso un Paese terzo non assicurante un adeguato livello di protezione può essere consentito nei seguenti casi:

a. Il titolare dei dati ha dato il proprio consenso in maniera non ambigua al trasferimento

b. Il trasferimento è necessario per l'esecuzione di un contratto tra il titolare dei dati e il responsabile del trattamento o per l'attuazione di misure pre-contrattuali adottate in risposta ad una richiesta avanzata dal titolare dei dati

c. Il trasferimento è necessario per la conclusione di un contratto nell'interesse del titolare dei dati tra il responsabile del trattamento e un soggetto terzo

d. Il trasferimento è necessario o legalmente richiesto in virtù di un rilevante interesse pubblico o per l'affermazione, esercizio o difesa di azioni legali

e. Il trasferimento è necessario al fine di proteggere un interesse vitale del titolare dei dati

f. Il trasferimento viene fatto da un registro che secondo le leggi o i regolamenti è diretto a fornire informazioni al pubblico e che è aperto alla consultazione da parte del pubblico in generale o da parte di qualsiasi persona che possa dimostrare un interesse legittimo nella misura in cui le condizioni previste dalla legge per la consultazione siano rispettate nella circostanza di specie.

La norma, stante il suo carattere derogatorio rispetto al principio generale, ha formato oggetto di un articolato parere da parte del Gruppo di lavoro ex art. 29. In particolare, l'intervento del Gruppo ex art. 29 si era reso necessario un funzione del rilevamento di diverse interpretazioni della norma, circostanza suscettibile di pregiudicarne l'uniforme applicazione a livello europeo. Inoltre, l'interpretazione particolarmente "blanda" che della norma veniva fatta presso alcuni Stati membri, unitamente alle divergenze con le quali gli stessi avevano trasposto ed attuato gli articoli 25 e 26 della direttiva, avrebbe potuto determinare il rischio di dare origine a situazioni di "forum shopping". Infine, era stato rilevato come fosse invalsa l'abitudine, presso molti responsabili del trattamento, di utilizzare il sistema di deroghe previsto dall'art. 26 come prima opzione, anche laddove la scelta era inappropriata.

Pertanto, la scelta di intervenire con un parere da parte del Gruppo di Lavoro ex art. 29 era dettata dall'esigenza di assicurare un'interpretazione il più possibile uniforme dell'art. 26.

In primo luogo è stato chiarito che le deroghe previste dall'art. 26 della Direttiva debbano essere interpretate in senso restrittivo, stante il loro carattere di eccezione rispetto alla disciplina generale. In quest'ottica, osserva il Gruppo di Lavoro, la logica è la stessa di quella che ispira il protocollo addizionale alla Convenzione 108. La relazione a tale protocollo recita infatti che "le parti hanno discrezionalità nel prevedere delle deroghe al principio di livello adeguato di protezione. Le disposizioni nazionali rilevanti devono in ogni caso rispettare il principio inerente la legge Europea secondo cui le clausole che prevedono eccezioni devono essere interpretate restrittivamente affinché l'eccezione non divenga la regola"[329].

Più in generale la regola della stretta interpretazione deriva chiaramente altresì dal case law dellaCorte Europea dei Diritti Umani che interpreta i diritti fondamentali in un modo alquanto ampio, ai sensi del "principe d'effet utile" della protezione offerta, con l'effetto di limitare il campo di applicazione delle deroghe a tale principio[330]

In secondo luogo il Gruppo di lavoro propende per la necessità che i responsabili dei trattamenti assicurino "adeguata protezione" in quante più situazioni sia possibile e di consentire il trasferimento sulla base delle deroghe di cui all'art. 26 par. 1 soltanto ove non siano concretamente

[329] Cf. report on the Additional Protocol to Convention 108 on the control authorities and crossborder flowsof data, Article 2(2)(a); this document can be accessed at: http://conventions.coe.int/Treaty/EN/Reports/Html/181.htm

[330] Si vedano in particolare le sentenza Delcourt (17 gennaio 1970) e Klass (6 settembre 1978).

applicabili le garanzie di cui all'art. 26 par. 2, ossia le clausole contrattuali standard o le *binding corporate rules*. Ciò soprattutto per quanto riguarda i trasferimenti di dati ripetitivi o strutturali.

Infine, il Gruppo di Lavoro ha espresso la considerazione che il trasferimento sulla base delle deroghe di cui all'art. 26 non deve mai portare ad una situazione in cui i diritti fondamentali possano essere violati. Molto opportunamente, infatti, il Gruppo di Lavoro evidenzia come il carattere derogatorio rivestito da queste norme riguardi esclusivamente il livello adeguato di protezione e non anche la regola secondo cui i diritti fondamentali debbano essere rispettati.

Tuttavia, si è anche riconosciuto che l'espansione del commercio a livello internazionale richiede in certe occasioni una certa flessibilità nei trasferimenti di dati, incluse le informazioni personali.

Ferme restando queste considerazioni di carattere generale il Gruppo di Lavoro,nel suo parere,ha preso posizione con riferimento a ciascuna singola ipotesi di deroga prevista dall'art. 26.

In primo luogo, per quanto riguarda il consenso, il Gruppo di lavoro insiste sul fatto che esso deve essere dato in forma esplicita affinché la deroga di cui all'art. 26 par. 1 lett. a) possa trovare applicazione. Tutte le situazioni in cui il consenso viene dato per implicito non possono rientrare nel campo di applicazione della deroga. Per tale ragione il consenso deve essere stato fornito in maniera libera e, per essere valido, deve essere fornito da una persona che ha avuto la possibilità di fare una scelta. Il consenso deve poi essere specifico ed informato. In particolare, il titolare dei dati deve essere compiutamente istruito in merito ala Paese di destinazione del flusso dei dati e dei rischi potenziali derivanti dal trasferimento

Per quanto riguarda i trasferimenti resi necessari per l'esecuzione di un contratto tra il titolare dei dati e il responsabile del trattamento, sebbene il campo di applicazione di tale deroga possa apparire potenzialmente molto ampio, il Gruppo di Lavoro ha specificato che, in pratica, essa dovrà essere limitata dal criterio della "necessità". Questa verifica sulla necessità richiede una connessione sostanziale e specifica ctra il titolare dei dati e la finalità del contratto. Analoghe considerazioni, in punto di necessità, riguardano la deroga prevista dall'art. 26 par. 1 lett. c) ove la valutazione di necessità deve attenere all'interesse del titolare dei dati e allo scopo del contratto.

Allo stesso modo, con riferimento all'eccezione di cui all'art. 26 par. 1 lett. d), Il gruppo di Lavoro ha precisato che la nozione di " rilevante interesse pubblico" può legittimare un trasferimento di dati verso un Paese terzo non assicurante un livello adeguato di protezione soltanto ove l'interesse pubblico venga individuato come tale da responsabili del trattamento situati in Europa. In quest'ottica il Gruppo di Lavoro, nell'opinione riguardante i trasferimento di dati PNR dei passeggeri[331], il gruppo di lavoro ha dato un'interpretazione restrittiva della nozione di "ragioni

[331] Opinion 6/2002

di rilevante interesse pubblico", rigettando l'uso di tale deroga al fine di legittimare il trasferimento dei dati PNR al Department of Homeland Security americano. Secondo il Gruppo di Lavoro, infatti, in primo luogo la necessità del trasferimento non era stata appurata e, in secondo luogo, non appariva accettabile che una decisione unilaterale di un paese terzo, sulla base di interessi pubblici specifici di quest'ultimo, potesse dare luogo a dei trasferimenti regolari ed in massa di dati protetti dalla Direttiva. Allo stesso modo, affinché un interesse pubblico possa legittimare un trasferimento di dati personali verso un paese terzo occorre che si tratti di un interesse "rilevante". Semplici, ma non importanti, considerazioni di interesse pubblico non valgono a legittimare un trasferimento.

L'art. 26 par. 1 lett. e) prevede invece la possibilità di dare luogo al trasferimento di dati al fine di proteggere un interesse vitale del titolare dei dati medesimi. Il gruppo di lavoro ha rilevato come tale eccezione debba essere interpretata nel senso di considerare come "interesse vitale" soltanto le situazioni di pericolo per la vita del titolare dei dati. Pertanto, importanti interessi di carattere finanziario, familiare o patrimoniale non potranno essere presi in considerazione alla luce dell'eccezione de quo.

L'ultima deroga attiene ai trasferimenti fatti da registri che, a norma di legge, sono aperti alla consultazione da parte del pubblico, purché siano rispettate le condizioni necessarie alla consultazione. In merito a tale ultima eccezione il Gruppo di Lavoro ha osservato come il trasferimento, sebbene avvenga a partire da un registro aperto alla consultazione del pubblico, i trasferimenti del contenuto di interi registri di intere categorie di dati ivi contenute non può essere ammesso.

5. Il trasferimento di dati personali verso Paesi terzi e self-regulation

Come si è illustrato nelle pagine precedenti l'art. 25 della Direttiva 95/46/CE richiede che l'adeguatezza del livello di protezione venga valutata alla luce di tutte le circostanze che soggiacciono al trasferimento dei dati. La disposizione in questione fa specifico riferimento non soltanto alle norme di legge vigenti nel Paese terzo ma anche alle "regole professionali e alle misure di sicurezza che vengono rispettate in quel paese". Pertanto,assumono particolare rilievo le norme di cd. *self regulation*, ossia quelle fonti di rango non legislativo che vengono generalmente adottate vuoi da singole aziende, vuoi da interi comparti industriali.

Sebbene non vi sia una definizione universale di self regulation, con tale termine generalmente si suole indicare quei set di regole sulla protezione dei dati che si applichino ad una pluralità di soggetti appartenenti alla medesima categoria professionale o industriale, ed il cui contenuto sia

stato determinato precipuamente dai membri della professione o del settore industriale interessato. Come osservato dal Gruppo di Lavoro siffatta definizione è suscettibile di includere tanto i codici volontari in materia di *data protection* elaborati da associazioni professionali o industriali di piccole dimensioni o scarsamente rappresentative, quanto quei complessi codici di etica professionale che siano, invece, applicabili ad intere professioni, quali medici e banche, che spesso hanno una forza quasi legislativa. Basti pensare, in questo senso, alle norme del Codice Deontologico che regola la professione di Avvocato in Italia, la cui natura di norme giuridiche è stata sancita dalle Sezioni Unite della Corte di Cassazione[332], superando così il precedente orientamento che attribuiva alle medesime valore contrattuale.

Ciò premesso, il Gruppo di Lavoro ha efficacemente osservato come, al fine di valutare il livello di protezione offerto da un regime di self-regulation, non si tratti tanto di verificare le dimensioni e la rappresentatività dell'associazione o dell'organo professionale in termini di numero di iscritti, quanto di misurarne la forza e la capacità di assicurare il rispetto delle regole e di imporre delle sanzioni. In ogni caso, si deve comunque ritenere che i codici di regolamentazione che riguardano intere professioni o interi comparti industriali offrono dei significativi vantaggi in termini di trasparenza e di chiarezza. Invero, dal punto di vista del consumatore, un comparto industriale o professionale altamente frammentato può risultare confuso. Allo stesso modo, evidenti problemi possono insorgere allorquando un'azienda trasferisce dati personali ad un'altra azienda che non sia soggetta al rispetto del medesimo codice di condotta. Per questi motivi, il Gruppo di Lavoro ha affermato come la valutazione circa l'adeguatezza del livello di protezione offerto da unn regime di self regulation debba essere valutata con particolare attenzione.

In quest'ottica, sempre secondo il Gruppo di Lavoro, la trasparenza del codice gioca un ruolo fondamentale, atteso che le relative norme dovranno essere formulate in un linguaggio chiaro ed offrire degli esempi concreti che ne illustrino il contenuto. Inoltre il codice dovrebbe proibire la divulgazione di dati a soggetti non membri che non sono governati dal codice stesso a meno che non vengano offerte adeguate garanzie.

Tre, sono dunque i criteri necessari affinché il livello di protezione dei dati offerto da un regime di self-regulation possa ritenersi adeguato. Innanzitutto vi deve essere un buon livello di osservanza delle norme. In questo senso molto dipenderà dalla trasparenza del codice, dagli sforzi dell'Associazione o dell'organo rappresentativo di divulgarne la conoscenza e di assicurarne il rispetto, dall'esistenza di sanzioni efficaci e dissuasive quali l'esclusione dalla categoria professionale in caso di mancato rispetto e cos' via. L'esistenza di un sistema sanzionatorio efficace

[332] Cassazione Civile Sezioni Unite Sentenza n. 26810 del 20 dicembre 2007

è, quindi, un elemento assai rilevante ai fini della valutazione del livello di protezione offerto dal codice.

Inoltre il sistema deve offrire sostegno ed aiuto ai titolari di dati mediante l'accesso ad un organo indipendente ed imparziale che assicuri il contraddittorio e decida sulle violazioni.

Infine, sempre secondo il Gruppo di Lavoro, il sistema deve prevedere degli appropriati meccanismi di riparazione in caso di mancata osservanza delle regole. I titolari dei dati devono, cioè, essere in grado di ottenere dei rimedi e compensazione dei danni subiti.

PARTE SECONDA

LA VICENDA SWIFT E L'ACCORDO TFTP II

1. La creazione del "Terrorist Finance Tracking Program"

A seguito degli attacchi dell'11 settembre 2001 gli Stati Uniti d'America, guidati dall'amministrazione Bush, hanno provveduto ad emanare numerosi provvedimenti legislativi tesi a rafforzare la sicurezza nazionale ed a fare fronte alla minaccia del terrorismo. Simili iniziative legislative hanno avuto eco anche negli ordinamenti delle altre democrazie occidentali, nonché presso gli Stati membri dell'Unione Europea.

In particolare, prima che Al Qaeda attaccasse i centri militari ed economici degli USA, le autorità federali non si erano mai poste il problema del finanziamento del terrorismo. I costi relativamente bassi necessari alla progettazione ed all'esecuzione degli attentati, unitamente alla convinzione che lo sceicco Usama Bin Laden finanziasse l'intera organizzazione jihadista attraverso la propria personale fortuna, avevano sino ad allora indotto gli Stati Uniti a dare priorità ad altre strategie di lotta al terrorismo[333].

Tuttavia, la facilità con la quale i terroristi dell' 11 settembre 2001 si servirono del sistema bancario per porre in essere la loro impresa, spinse le autorità federali a ricredersi sul punto. Infatti, quando i dirottatori giunsero negli Stati Uniti, aprirono dei conti correnti bancari intestati a loro nome presso una filiale della Sun Trust in Florida, ove vi trasferirono importi varianti dai 5.000 $ ai 70.000 $ provenienti da banche degli Emirati Arabi Uniti e dalla Germania, per un totale di 130.000 $[334] . Tale importo costituì il capitale necessario per l'esecuzione materiale dell'attentato[335].

Quando tutto ciò venne alla luce, apparve subito evidente che la strategia pregressa degli USA, di combattere il finanziamento del terrorismo facendo ricorso alle comuni disposizioni in materia di riciclaggio del denaro, fosse del tutto inadeguata[336]. Infatti, sebbene le disposizioni in materia di anti-riciclaggio consentano la confisca dei beni, esse presuppongono comunque l'avvenuta commissione un reato, elemento che risulta, invece, spesso assente nel caso del terrorismo, ove la commissione del reato si verifica, semmai, in un momento successivo. Inoltre, se le attività

[333] Laura K. Donohue, "*Anti –Terrorist Finance in the United Kingdom and the United States*", 27 MICH J. INT'L L. 303,349 (2006)
[334] Jeff Gerth & Judith Miller, "*A Nation Challenged: Money Trail, US makes Inroads in isolating funds of terrorist groups"*, NY Times Nov. 5, 2001, at. A1
[335] Idem
[336] Adrienne Margolis "*Swift Response to preventing terrorist financing*", in Int Bar News 62 no. 1 F 2008 p. 12-15

economiche legate al crimine organizzato generalmente mirano a ripulire i proventi di attività illecite, con gli attentati del 11 settembre 2001 il terrorismo internazionale aveva dimostrato di essere perfettamente in grado di fare ricorso a fondi leciti per finanziare azioni criminali[337]. Era divenuto necessario, dunque, agli occhi delle autorità federali e dell'amministrazione Bush, togliere al terrorismo la possibilità di finanziarsi[338].

Ciò premesso, in data 23.01.2001, ossia due settimane dopo gli attacchi che rasero al suolo le Twin Towers ed un'intera sezione del Pentagono, il Presidente Bush adottava l'Executive Order 13224 recante "*Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit or Support Terrorism*" [339].

Tale atto, con il quale si proclamava lo stato di emergenza nazionale, autorizzava il Presidente a fare ricorso ai poteri dell'*"International Emergency Economic Powers Act" (IEEPA)* [340] al fine di congelare i beni di persone fisiche o giuridiche sospettate di terrorismo e di proibire qualsiasi ulteriore transazione con o in favore dei terroristi, ovvero di soggetti che sostengono il terrorismo. Inoltre, grazie alle disposizioni del Titolo III del PATRIOT Act[341], venivano ulteriormente ampliati i poteri dell'esecutivo ai sensi del sopraccitato IEEPA. Nello specifico, veniva accresciuta la capacità del governo di obbligare le istituzioni finanziarie a cooperare con le autorità di pubblica sicurezza, sotto pena di congelamento dei loro beni ai sensi dell'Executive Order 13224.

E' proprio sulla base di tale Executive Order che il Dipartimento del Tesoro Americano, tramite l'Office for Foreign Assets Control (OFAC) iniziava, di concerto con la CIA, il cd. "*Terrorist Finance Tracking Program"* TFTP. Sulla base di tale iniziativa, dunque, che durante i primi anni venne condotta in maniera assolutamente segreta, il Dipartimento del Tesoro, forte dei poteri conferitigli dal Presidente tramite l'Executive Order 13224, iniziò ad emettere delle "*administrative subpoenas*" nei confronti delle istituzioni finanziarie operanti sul territorio statunitense al fine di costringerle a fornire tutte le informazioni in loro possesso con riferimento alle transazioni bancarie da esse gestite.

Nel diritto americano il termine "*subpoena*" indica generalmente un comando che il giudice, d'ufficio o su richiesta di una della parti, rivolge ad un determinato soggetto al fine di indurlo a

[337] Erich Lichtblau & James Risen, "*Bank Data Sifted in Secret. US Secretly tracks global bank data"*, L.A. Times, June 23, 2006 at A1.
[338] Idem
[339] Executive Order 13,224, 66 Fed. Reg. 49,079 (23.01.2001) recante "*Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit or Support Terrorism*".
[340] International Emergency Economic Powers Act, 50 U.S.C. § 1702(a) (1)(B)(2000).
[341] PATRIOT Act, ovvero "*Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*", Pub L No. 107-56, 115 Stat. 272 (2001) codificato in 50 U.S.C. § 1861.

tenere un determinato comportamento sotto minaccia di una sanzione (da qui la derivazione latina del termine *sub poena*) che, nei casi più gravi è qualificabile come reato[342].

Attraverso una *subpoena,* dunque, un giudice americano può ordinare ad un testimone di comparire in udienza, ovvero ad una società di fornire determinate informazioni. In altri termini, mediante lo strumento della *subpoena* il giudice americano è in grado di ottenere, in maniera assai duttile e senza eccessivi formalismi, risultati analoghi a quelli che, nei sistemi europei, risultano conseguibili mediante i provvedimenti di natura urgente o cautelare.

Giova, altresì, osservare che, oltre all'autorizzazione del giudice, generalmente le *subpoena*s, possono essere emesse soltanto in presenza di determinati requisiti. Ad esempio nella giustizia penale l'emissione di una *subpoena* è subordinata alla presenza della "*probable cause*"[343], ossia alla sussistenza dei gravi indizi di colpevolezza. Più in generale le *subpoenas* richiedono l'equivalente del "*fumus boni juris*". Tuttavia, le *administrative subpoenas* emesse dal Dipartimento del Tesoro si differenziano notevolmente da quelle ordinarie in quanto, oltre a non necessitare dell'autorizzazione del giudice, incontrano come unico limite il requisito della *"ragionevolezza"* stante il loro carattere di provvedimento amministrativo[344].

Mediante l'utilizzo di tale strumento e dell'efficacia deterrente delle relative sanzioni, dunque, il Dipartimento del Tesoro iniziò a richiedere e ad ottenere con particolare facilità la comunicazione, da parte delle istituzioni finanziarie operanti nel territorio statunitense, di tutte le informazioni riguardanti le transazioni finanziarie da esse condotte per finalità di lotta al terrorismo. In particolare, l'oggetto di tali *subpoenas* si caratterizzava per essere particolarmente ampio, in quanto queste venivano emesse per qualsiasi transazione che poteva avere un legame con il terrorismo, con riferimento a un numero X di paesi e giurisdizioni, ed in un periodo Y di tempo variabile. Inoltre, dette richieste di informazioni potevano avere per oggetto le informazioni relative alle transazioni bancarie condotte all'interno degli USA, ma anche verso gli USA, al di fuori degli USA e persino all'interno della UE[345].

Ciò premesso, a livello mondiale, le transazioni finanziarie circolano attraverso un circuito gestito da una società avente sede in Belgio, ma dotata di uffici sparsi in almeno altri sedici paesi, denominata *Society for Worldwide Interbank Financial Telecommunication* (SWIFT).

SWIFT non è altro che un network creato nel 1973 da un pool di 239 banche di 15 diversi paesi[346]. Esso viene oggi supervisionato dalla Federal Reserve Americana, dalla Bank of England,

---

[342] Fanchiotti Vittorio "*Voce "Processo Penale Statunitense (annali II-1 2008*)" in Enciclopedia del Diritto, Giuffré

[343] Katherine Scherb*, "Comment, Administrative Subpoenas for Private Financial Records:What Protection for privacy does the fourth amendment afford?",* WIS L. REV. 1075, 1075-85 (1996)

[344] United States v. Powell, 379 U.S. 48, 57-58 (1964)

[345] "*Swift Statement on compliance policy*" pubblicato su http://www.swift.com/index.ctm?item_id=59897

[346] Swift.com, SWIFT History, http://www.swift.com/index.cfm?item_id=1243 aggiornato al 25.09.2012

dalla Banca Centrale Europea e dalla Bank of Japan oltre che dalla Banca Nazionale Belga. Il circuito SWIFT mette oggi in comunicazione tutte le più grandi istituzioni finanziarie del globo con finalità di scambio di informazioni relative a pagamenti e transazioni finanziarie di ogni genere.

Come si potrà notare SWIFT non gestisce denaro, bensì il trattamento delle istruzioni criptate di trasferimento e di conferma delle operazioni bancarie internazionali. Attraverso questi messaggi criptati sono solite transitare attraverso il circuito SWIFT informazioni riguardanti le cifre trasferite, i metodi di trasferimento, l'identità delle parti dell'operazione e le banche partecipanti[347]. Dette informazioni, all'epoca dei fatti, venivano conservate tanto nei server europei della società, quanto nel server situato sul territorio statunitense per un periodo di 120 giorni per finalità di backup[348].

In altre parole le banche dati della SWIFT immagazzinavano (e tutt'ora conservano) nomi, indirizzi, numeri di conto corrente dei mittenti e dei destinatari di bonifici internazionali tra banche ed altri enti, costituendo così una fonte di informazioni particolarmente appetibile per i funzionari federali incaricati di seguire i flussi transfrontalieri di denaro per finalità di sicurezza interna[349]. Ogni giorno, attraverso il circuito SWIFT, circolano le informazioni relative a milioni di transazioni finanziarie e, conseguentemente, milioni di dati ed informazioni personali relativi ad altrettanti cittadini ed imprese europee[350]. E' stato calcolato, ad esempio che, solo nel 2006, SWIFT gestiva i flussi di informazioni relativi ad 11 milioni di transazioni finanziarie giornaliere tra 7.800 banche in 200 paesi[351]. Attualmente, circa 8000 istituzioni finanziarie in 206 paesi fanno uso dei servizi Swift

All'epoca dell'emissione della prima *subpoena* amministrativa nell'Ottobre 2001, la società SWIFT aveva una sede operativa in Virginia, negli Stati Uniti, nel cui database veniva immagazzinata una copia dei dati relativi alle transazioni scambiate. Tale elemento di territorialità fondava la giurisdizione americana ai fini dell'emissione delle *subpoenas* amministrative. Fino alla conclusione del primo accordo con l'Unione Europea, il Dipartimento del Tesoro avrebbe emesso 63 ulteriori *subpoenas*.

Le prime *subpoenas* di cui fu destinataria la SWIFT si caratterizzavano per il fatto di essere dirette ad ottenere informazioni in merito alle informazioni che la società aveva trasferito nel suo centro operativo negli USA. Esse, tuttavia, non individuavano specifici soggetti ovvero transazioni in particolare, assumendo perciò un contenuto meramente esplorativo[352].

---

[347] SWIFT Statement Francis Vanbever, Chief Financial Officer, European Parliament Hearing Oct. 4 2006 reperibile su http://www.swift.com/index/index.cfm?item_id=60670 aggiornato al 25.09.2012

[348] SWIFT Statement cit sub nota 14

[349] Brand C. "*Belgian PM: Data Trasfer Broke Rules"* Associated Press. Reperibile su http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html. Consultato il 25.09.2012

[350] Idem

[351] Ibidem

[352] Santolli Justin, nota 287

Proprio per questo motivo, già nel 2003, la SWIFT, che aveva sino ad allora cooperato in maniera assolutamente diligente con le autorità federali, iniziava a manifestare la propria riluttanza a dover partecipare ad un'iniziativa che, oltre ad essere altamente confidenziale, non prevedeva neppure una data finale e sulla quale mancava qualsiasi forma di controllo da parte di un'autorità indipendente. Veniva quindi indetta una riunione tra i suoi alti funzionari, il presidente della Federal Reserve Aland Greenspan, ed il direttore dell'FBI Robert Mueller al fine di venire incontro alle preoccupazioni della società[353].

Tra le concessioni che il *Department of Treasury* fece alla società figurava una maggiore delimitazione della nozione di terrorismo di cui all'Executive Order 13224. Allo stesso modo il Dipartimento del Tesoro rassicurava la SWIFT sul fatto che avrebbe perseguito soltanto individui legati ad una indagine attuale sul terrorismo. Inoltre, il governo USA e la SWIFT concordarono di dare mandato ad una società di consulenza americana, Booz Allen Hamilton, di supervisionare le operazioni del TFTP, al fine di assicurare una qualche forma di controllo esterno circa la legittimità delle richieste.

2. La rivelazione della stampa e le reazioni delle istituzioni europee

Il 23 giugno 2006 diversi grandi giornali americani tra cui il New York Times, il Los Angeles Times ed il Wall Street Journal pubblicavano la notizia dell'esistenza dell'iniziativa segreta della CIA e del Dipartimento del Tesoro conosciuta, appunto, sotto il nome di *Terrorist Finance Tracking Program (TFTP).* L'opinione pubblica americana veniva, così, a conoscenza del fatto che il Dipartimento del Tesoro e l'intelligence nazionale stavano in pratica sorvegliando, da oramai quattro anni, i movimenti bancari dei cittadini e delle aziende nell'intento (dichiarato) di combattere il terrorismo.

La rivelazione provocava una reazione tutto sommato limitata in seno alla società statunitense, oramai abituata all'irrigidimento dei controlli post 11 settembre. Non mancarono, tuttavia, le critiche al TFTP. Secondo parte della dottrina, infatti, l'utilità dell'iniziativa pareva tutto sommato, dubbia, atteso che la maggior parte delle cellule terroriste erano solite autofinanziarsi. Allo stesso modo, veniva osservato anche che il TFTP controllava i flussi internazionali di denaro ma non anche le operazioni più semplici condotte su territorio nazionale, quali i prelievi dagli ATM. Inoltre,

[353] Lichtblau & Risens, nota 337

la dottrina statunitense si è chiesta se tale iniziativa violasse il Quarto emendamento contro le irragionevoli perquisizioni e sequestri[354].

In ogni caso, nonostante le critiche formulate nei suoi confronti, il TFTP godeva, negli USA, di un solido consenso da parte delle istituzioni. Infatti, sei giorni a seguito della rivelazione della stampa la *House of Representatives* degli Stati Uniti adottava una risoluzione ove esprimeva il proprio supporto per il programma, nonché la convinzione che esso fosse assolutamente compatibile con le leggi applicabili[355]. Allo stesso modo, il Presidente George W. Bush dichiarava espressamente che gli USA non avrebbero mai rinunciato al TFTP[356], la cui utilità come strumento nella lotta al terrorismo presentava, a suo dire, un valore incalcolabile.

Il Governo USA, dunque, sceglieva di difendere apertamente la legittimità del TFTP, non soltanto in quanto le relative misure trovavano fondamento in una legge emanata dal Congresso, la IEEPA, ma anche in considerazione dello Stato di emergenza nazionale in cui evrsavabnio che giustificava l'adozione di misure eccezionali[357]. I sostenitori del TFTP inoltre, osservavano come la prova ulteriore della legittimità del programma si ricavasse dal fatto che le varie *subpoenas* amministrative non erano mai state contestate in giudizio da parte della SWIFT o delle altre istituzioni finanziarie coinvolte[358]. Allo stesso modo, i partigiani del TFTP sottolineavano come esso si fosse rivelato indispensabile ai fini dell'arresto avvenuto in Thailandia del terrorista Hambali, l'ideatore dell'attentato di Bali del 2002, nonché quello avvenuto a New Yorl di Uzair Pachara con l'accusa di aver finanziato Al Qaeda tramite una banca di Karachi[359].

Ciò premesso, se la notizia che il Governo Federale americano stava sostanzialmente spiando le transazioni commerciali dei cittadini europei da più di cinque anni suscitò delle reazioni tutto sommato modesta in seno all'opinione pubblica americana, essa suscitò invece ampio scandalo in Europa, se non altro per il fatto che la Banca Centrale Europea, in compagnia delle principali banche nazionali europee, erano perfettamente al corrente di quanto stava avvenendo[360].

In particolare, la BCE, che figura tra le banche che supervisiona la SWIFT, respingeva le critiche di non aver fatto nulla per proteggere la privacy degli europei, affermando che la decisione della società di fornire le informazioni agli USA era al di là dei suoi poteri di controllo.

---

[354] Katherine Scherb , nota 343
[355] Cfr. H.R. 896, 109th Cong. (2006)
[356] Erich Lichtblau, Controls on bank-data spying impress civil liberties board" NY Times June 29, 2007 at A26
[357] Idem
[358] Patrick M. Connorton "Tracking terrorist financing through SWIFT: when U.S. subpoeans and foreign privacy law collide" Fordham Law Rev 76 n. 1 O 2007
[359] Erich Lichtblau, nota 356
[360] Marc-Antoine Ledieu "CNIL – *Surveillance des transferts bancaires européens par les autorités américaines : vers une remise en cause des garanties négociées*" in Communication Commerce électronique n° 10, Octobre 2009, alerte 129

In particolare il Presidente della BCE Jean Claude Trichet dichiarò al Parlamento Europeo che le banche centrali del G-10 "*did not give SWIFT any blessing in relation to its compliance with these subpoenas, In fact, we could not have given any such authorisation even if we had wanted to, as this fell outside our competence. Therefore, SWIFT remained solely responsible for its decisions*"[361]

Tuttavia, in un comunicato stampa Peter Hustinx, presidente del Garante Europeo per la protezione dei dati replicò che "*come qualsiasi altra banca, la BCE non può sfuggire ad una qualche forma di responsabilità con riferimento al caso SWIFT che determinato la violazione della fiducia e delle vite private di milioni di persone. L'accesso segreto, abituale e massiccio da parte delle autorità di paesi terzi alle informazioni bancarie è inaccettabile. La comunità finanziaria dovrebbe quindi prevedere dei sistemi di pagamento che non violino le leggi europee sulla protezione dei dati*"[362].

Invero, secondo il Garante per la protezione dei dati, la BCE nel contesto dei sistemi di pagamento aveva una posizione di triplice responsabilità. Essa è infatti supervisore, utilizzatrice nonché *policy maker* per quanto riguarda i servizi della SWIFT. Invero, in quanto parte delle banche che supervisionano le attività della SWIFT la BCE ha quantomeno dei poteri di *moral suasion* che, benché non vincolanti, avrebbero potuto essere impiegati al fine di evitare delle violazioni al regime normativo di protezione dei dati e assicurare che le autorità competenti fossero tempestivamente informate. La BCE ha inoltre, qualche responsabilità in merito a come i dati dei suoi clienti sono trattati da SWIFT. Invero, agendo efficacemente come "*joint controller*" ai sensi della Direttiva 95/46/CE, la BCE avrebbe dovuto assicurare il pieno rispetto delle regole sulla protezione dei dati per conto dei suoi clienti Allo stesso modo, la BCE ha un ruolo determinante nell'elaborazione delle politiche nel campo dei sistemi di pagamento europei. In tale veste dovrebbe assicurare che l'architettura di tali sistemi di pagamento non permetta che le informazioni sui pagamenti vengano trasferiti a paesi terzi in violazione delle leggi sulla protezione dei dati[363].

Dal canto suo il Parlamento Europeo, in data 6 luglio 2006, emanò una Risoluzione con la quale chiese agli Stati membri di verificare che non vi fossero lacune legislative a livello nazionale e che la legislazione europea in materia di protezione dei dati coprisse anche le banche centrali[364]. Nella sua risoluzione il Parlamento esprimeva, altresì, grande preoccupazione circa lo scopo del

[361] Jean-Claude Trichet: Discorso del Presidente della BCE dinanzi al Parlamento Europeo sull'intercettazione dei dati relative ai trasferimenti bancari dal sistema SWIFT ai servizi segreti americani.
[362] Comunicato stampa del 1.02.2007 "*EDPS calls on ECB to ensure that European payment systems comply with data protection law*", reperibile sul sito www.edps.europa.eu aggiornato al 25.09.2012
[363] Id. Sub nota 13
[364] European Parliament resolution on the interception of bank transfer data form the SWIFT systeem by the US secret services (P6_TA-PROV(2006)(0317)

trasferimento di dati verso il Dipartimento del Tesoro statunitense, disapprovava la conduzione di qualsiasi operazione segreta sul territorio dell'Unione Europea che potesse coinvolgere la privacy dei cittadini europei ed esprimeva la propria profonda costernazione per il fatto che tali operazioni avessero luogo senza che i cittadini europei o i loro legittimi rappresentanti ne fossero stati informati[365]. Da ultimo, la risoluzione invitava gli USA e i suoi servizi di sicurezza ad agire secondo uno spirito di leale cooperazione e di notificare ai loro alleati tutte le operazioni di sicurezza che intendevano svolgere sul territorio dell'Unione Europea[366].

Anche il Presidente del Gruppo di Lavoro ex art. 29, annunciava che le autorità europee sulla protezione dei dati avevano deciso di coordinare le proprie attività, giungendo ad una prima discussione plenaria il 26-27 settembre 2006[367]. In tale data, l'Autorità Belga per la Protezione dei Dati aveva già pubblicato un proprio parere, secondo cui il trasferimento di dati personali da parte di SWIFT agli USA era avvenuto in violazione della legge belga del 8 dicembre 1992 concernente "*la protezione della privacy con riferimento al trattamento di dati di una determinata natura*"[368].

In particolare la Commissione belga catalogava SIWFT come un "*data controller*" e non come un "*data processor*" distinzione che, a norma della Direttiva 95/46/CE comporta maggiori responsabilità[369]. Allo stesso modo l'Autorità belga evidenziava il fatto che SWIFT aveva violato diverse disposizioni fondamentali relative agli obblighi di informazione, limitazione dello scopo del trattamento e trasferimento verso paesi terzi, affermando che SWIFT aveva condotto una "*hidden, long term violation of the fundamental european principles as regards data protection,* che si era sostanziata nel trasferimento di dati personali verso un paesi con inadeguata protezione della privacy, segnatamente gli USA. Infatti, sebbene l'Autorità belga ammise che SWIFT avesse un "interesse legittimo" a rispettare le *subpoenas* americane, ciò non avrebbe mai potuto giustificare una violazione sistematica e su larga scala dei principi fondamentali europei sulla protezione dei dati.

Anche il Gruppo di Lavoro ex art. 29 esaminò da vicino la vicenda SWIFT e nell'ottobre 2006 ed emise un proprio parere nel quale giungeva alle seguenti conclusioni[370].

---

[365] Cfr. Risoluzione del Parlamento Europeo cit. sub nota 22

[366] Cfr. Risoluzione del Parlamento Europeo cit. sub nota 22

[367] Article 29 Working Party press releases: Press release of the Article 29 Working Party on Swift case of 28/7/2006 http//:ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_28_07_06_en.pdf; press releass on the SWIFT case of 27.09.2006 .
http//:ec.europa.eu/justice_home/fsj/privacy/news/docs/PR_SWIFT_Affair_26_09_06_en.pdf

[368] http://privacycommission.be/communiqu%E)s/AV37-2006.pdf

[369] Royaume de Belgique Commission de la Protection de la Vie Privée Opinion no. 37/2006 *"Opinion on the transfer of personal data by the CDRL SWIFT by Virtue of UST (OFAC) Subpoenas 26 (2006)"* reperibile su http://www.privacycommission.be/communiqu%E9s/opinion_37_2006.pdf. aggiornato al 25.09.2012

[370] Comunicato stampa del 23.11.2006 recante "Press release on the SWIFT case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial

Innanzitutto, i trasferimenti di dati personali dal circuito SWIFT verso gli USA erano governati dalla legge belga, stato ove SWIFT aveva la propria sede, indi erano soggetti ai principi di cui alla Direttiva 95/46/CE. Allo stesso modo sia SWIFT che le banche che utilizzavano i suoi servizi avevano violato la Direttiva 95/46/CE, sebbene con differenti gradi di responsabilità.

Il gruppo di Lavoro ex art. 29 osservava che ai sensi dell'art. 6 della Direttiva i dati personali devono essere trattati con lealtà e in maniera legittima; essi devono essere raccolti per scopi specifici, espliciti e legittimi e non possono essere trattati per finalità incompatibili con quelle per i quali sono stati raccolti. In quest'ottica il trasferimento di dati dal circuito SWIFT al Dipartimento del Tesoro USA ammontava ad un "trattamento ulteriore" non compatibile con gli scopi commerciali per i quali i dati erano stati raccolti ai sensi della direttiva. Invero, anche la giurisprudenza della Corte di Giustizia aveva avuto modo di affermare, nelle cause riunite C-465/00, C-138/01 e C-139/01 Rechnungshof/Lauermann del 20 maggio 2003 che la comunicazione di dati originariamente raccolti per finalità "economiche" a soggetti terzi, incluse le autorità pubbliche, "*costituisce un'ingerenza ai sensi dell'art. 8 della CEDU*" e che eventuali deroghe al principio della limitazione dello scopo previste dalla Direttiva sulla protezione dei dati devono essere conformi all'art. 13 della medesima e, pertanto, "*giustificate dal punto di vista dell'art. 8 della CEDU*". (cfr. punto 68 della decisione Rechnungshof).

Allo stesso modo il Gruppo di Lavoro osservava come né SWIFT né le istituzioni finanziarie coinvolte avessero informato i titolari dei dati dell'avvenuto trattamento dei loro dai e del loro trasferimento verso gli USA come richiesto dagli artt. 10 e 11 della Direttiva. Trasferimento che, nell'ottica della Direttiva, non poteva essere giustificato alla luce dell'art. 25, non offrendo gli USA un adeguato livello di protezione, né ricadere sotto alcuna delle deroghe di cui all'art. 26.

Le misure di controllo poste in essere da SWIFT non potevano rimpiazzare in alcun modo la supervisione da parte di un'autorità indipendente che poteva essere fornito da parte delle autorità nazionali di cui all'art. 28 della Direttiva.

Infine il Gruppo di Lavoro ex art. 29 stigmatizzò il fatto che, anche durante la lotta al terrorismo, i diritti fondamentali devono rimanere garantiti[371].

La società belga si trovò dunque ben presto tra l'incudine e martello, ossia tra le pressioni dell'autorità amministrativa americana per ottenere le informazioni sotto minaccia di pesanti sanzioni e il diritto degli Stati membri dell'Unione Europea che, sulla scorta della Direttiva

---

Telecommunications" (SWIFT) reperibile sul sito http://ec.europa.eu/justice/policies/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf aggiornato al 25.09.2012

[371] Cfr. Parere 10/2006 dell Gruppo di Lavoro ex art. 29: On the processing of personal data by the society for worldwide interbank financial telecommunication, reperibile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.

95/46/CE, vietavano il trasferimento di dati personali verso paesi non aventi un adeguato livello di protezione quali appunto gli Stati Uniti.

Nel giugno del 2007, dopo mesi di pubblica discordia, l'Unione Europea, sotto la guida della presidenza tedesca e l'amministrazione Bush, raggiunsero un accordo sulle garanzie addizionali che gli Stati Uniti avrebbero dovuto aggiungere al TFTP al fine di ottenere l'approvazione degli alleati europei[372]. A tal fine il Dipartimento del Tesoro diede un set di "*representations*" unilaterali circa i controlli e le garanzie che governano la gestione utilizzo e disseminazione di dati ai sensi del TFTP. In particolare, il Dipartimento del Tesoro assicurava che avrebbe sottoposto i dati a trattamento esclusivamente con finalità di lotta e prevenzione del terrorismo, e che avrebbe cancellato i dati che non sarebbero serviti a tale scopo[373]. Tale accordo pose fine ai dibattiti relativi al caso SWIFT almeno fino a quando la società non decise di smantellare il proprio centro operativo negli USA e di immagazzinare i propri dati in Olanda.

3. La conclusione del primo accordo TFTP. Il veto del Parlamento europeo

Come si accennava poc'anzi, alla fine del 2009 la SWIFT, in riscontro alle preoccupazioni espresse dalle istituzioni democratiche europee, smetteva di immagazzinare i duplicati dei dati relativi alle transazioni inter-bancarie provenienti Spazio economico Europeo nel suo server in Virginia, disponendone la registrazione esclusiva presso i server situati in Svizzera ed in Olanda. Tale scelta determinava, sostanzialmente la sottrazione dei dati di messaggistica finanziaria riguardanti lo spazio economico europeo al raggio d'azione delle *subpoenas* del Dipartimento del Tesoro Americano e spingeva gli USA, che intendevano continuare a percepire detti dati per le finalità di cui al TFTP, a dover cercare un accordo con l'Unione Europea[374].

Il 27 luglio 2009 i 27 ministri degli Affari Esteri degli Stati membri davano mandato alla Commissione Europea e alla Presidenza Svedese dell'Unione di negoziare un accordo *ad interim* con gli Stati Uniti al fine di dare accesso a questi ultimi ai dati bancari SWIFT. L'accordo in questione sarebbe dovuto durare fino all'entrata in vigore del Trattato di Lisbona.

[372] Comunicato Stampa USA to take account of EU data protection principles to process data received from SWIFT (28.06.2007) reperibile su http://europa.eu/rapid/pressReleasesAction.dp?reference=IP/07/968&format=HTML&aged=0&language=EN&guiLanguage=en aggiornato al 25.09.2012

[373] André PRÜM "*Bataille politique autour de SWIFT : la lutte contre le terrorisme doit compter avec le respect de la vie privée*", in Revue de Droit bancaire et financier n° 3, Mai 2010, alerte 9

[374] Idem

Alla procedura di adozione della decisione, che non implicò alcuna approvazione parlamentare a livello nazionale o europeo, venne impresso un ritmo accelerato. Invero il Vice Presidente della Commissione Jacques Barrot ed il Consiglio Europeo miravano a finalizzare l'accordo prima dell'entrata in vigore del Trattato di Lisbona, eliminando così il Parlamento dal processo decisionale. Parte della dottrina ha fortemente criticato un simile atteggiamento, evidenziando come ironicamente la Svezia, che si è sempre vantata di essere campionessa della democrazia partecipativa si collocava ora "*alla testa di un branco di burocrati Europei, non eletti e stra-pagati, nell'intento escludere i rappresentanti legittimi dei cittadini europei dai processi di negoziato e di voto*"[375].

Secondo il testo dell'accordo, l'Unione Europea avrebbe permesso alla SWIFT di condividere il nome, numero di conto, indirizzo, numero nazionale di identificazione e altri dati personali con le autorità statunitensi nel caso di sospetto che la persona in questione fosse in qualsiasi modo implicata in attività di terrorismo. La richiesta di informazione doveva essere ritagliata nella maniera più precisa possibile al fine di evitare che una quantità eccessiva di dati divenisse oggetto di valutazione da parte polizia e dai funzionari di intelligence. Tuttavia, laddove il fornitore dei dati si fosse rivelato incapace di identificare i dati richiesti per questioni tecniche, allora tutti i dati potenzialmente rilevanti avrebbero dovuto essere trasmessi in massa allo Stato richiedente. I dati trasmessi sarebbero stati custoditi dagli USA fino a cinque anni prima di essere cancellati.

L'accordo prevedeva che gli USA non sarebbero stati autorizzati a condividere i dati europei con paesi terzi e le transazioni tra paesi UE non sarebbero state monitorate. L'accordo iniziale doveva durare per nove mesi, con decorrenza dal 1 febbraio 2010 con l'ottica di stillare un accordo più durevole alla sua scadenza.

Il Consiglio decideva di accelerare i tempi della stipula dell'accordo al 30 novembre 2009, suscitando le ire del Parlamento Europeo, poiché appariva evidente che la manovra era diretta a far entrare in vigore il testo prima della Riforma di Lisbona, privando così il Parlamento dei suoi eguali poteri decisionali e di veto nell'area della giustizia e degli affari interni.

Soltanto l'opposizione di alcuni parlamenti nazionali fece si che il testo dovette alla fine essere deciso con la procedura di co-decisione. Tuttavia, sebbene il Presidente del Parlamento Europeo avesse chiesto al Consiglio e alla Commissione di riferire il testo in assemblea al fine di dare tempo al Parlamento di studiare l'accordo, la Presidenza Spagnola finse un ritardo adducendo motivi di traduzione e annunciò che il testo sarebbe stato trasmesso all'assemblea il 25 gennaio 2010. Il Parlamento scoprì dunque che il testo dell'accordo era già stato pubblicato sulla Gazzetta Ufficiale

[375] Sylvia Kierkegaard "*US War on terror EU swift(ly) signs blank cheque on EU data*", in Computer Law & Security Law Review 27 (2011) 451 - 464

il 13 gennaio[376] e che, con ogni evidenza, la scusa del ritardo era stata pianificata per evitare che il Parlamento, la cui riunione plenaria era prevista per l'8-11 febbraio, potesse raggiungere una decisione definitiva prima dell'entrata in vigore provvisoria dell'accordo del 1 febbraio 2010. Il Consiglio e la Commissione avevano così beffato il Parlamento, l'accordo *ad interim* entrava provvisoriamente in vigore per nove mesi decorsi i quali avrebbe dovuto essere rimpiazzato con un nuovo accordo.

Secondo la dottrina, l'accordo *ad interim* del 30 novembre 2009 presentava diverse lacune. Esso, infatti, si fondava su di una nozione di lotta al terrorismo i cui confini, nella legislazione americana, erano alquanto labili. Ciò faceva si che la trasmissione dei dati non corrispondesse ad uno scopo determinato con un grado di precisione necessaria al fine di permettere un efficace controllo di opportunità[377].

Allo stesso modo, l'accordo sembrava travalicare i confini del principio di proporzionalità che, invero, costituisce una condizione essenziale per qualsiasi ingerenza nel rispetto dei diritti fondamentali. Come stabilito dalla Corte EDU, infatti, "l*e pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques (...). Les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction (...). Dans le contexte de l'article 8, cela signifie qu'il faut rechercher un équilibre entre l'exercice par l'individu du droit que lui garantit le paragraphe 1 et la nécessité, d'après le paragraphe 2, d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble*"[378] Allo stesso modo la Corte insiste sul fatto che "*des transferts massifs et indifférenciés de données ne satisfont certainement pas à cette exigence*"[379]. Orbene, ciò è proprio quello che tendeva ad autorizzare l'accordo *ad interim*, nella misura in cui il sistema non permetteva apparentemente di ricercare dei dati in maniera obiettiva ma soltanto la comunicazione di pacchetti di informazioni riguardanti a delle intere serie di transazioni[380].

Inoltre, l'accordo non prevedeva le garanzie indispensabili al fine di prevenire e riparare degli eventuali abusi. Cosicché esso mancava di organizzare con sufficiente precisione i diritti di accesso, di rettifica e di ricorso della persona interessata, di fissare la durate della conservazione dei dati o di

[376] Cons. UE, déc. n° 2010/16/PESC/JAI, 30 nov. 2009, relative à la signature, au nom de l'Union européenne, de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis d'Amérique aux fins du programme de surveillance du financement du terrorisme : JOUE n° L 8, 13 janv. 2010, p. 9 à 16
[377] André PRÜM, nota 373
[378] Cfr. Corte Edu, sentenza sul ricorso n° 5029/71 del 6 settembre 1978, Klass et a. c/ Germania.
[379] Cfr. Corte Edu, sentenza sul ricorso n° 12661/87 del 25 febbraio 1993, Miailhe c/ Francia
[380] André PRÜM, nota 373

instaurare le procedure di controllo per vegliare al rispetto della finalità del trasferimento[381]. In definitiva, ciò che rilevava la dottrina, era che, come peraltro affermato dalla Corte Europea dei Diritti Umani[382], uno Stato di diritto non può esimersi dal rispettare i diritti fondamentali di ciascun cittadino, non potendo la lotta al terrorismo condurre all'utilizzo di mezzi che minino i fondamenti di una società democratica[383].

Successivamente, come prevedibile, in data 4 febbraio 2010 la Commissione per le libertà civili del Parlamento Europeo respinse il testo. In una lettera indirizzata alla Commissione il Garante Europeo per la Protezione dei dati sottolineava come le misure previste dal TFTP fossero altamente invasive della privacy. In particolare, vi dovevano essere delle ragioni forti affinché tali misure intrusive fossero da considerarsi necessarie e proporzionate. Orbene, nell'ottica del Garante le prove fornite non dimostravano interamente la necessità ed il reale valore aggiunto con rispetto a misure maggiormente specifiche di combattimento al terrorismo. Nell'accordo TFTP diversamente da quanto avviene nel PNR non vi era alcun elemento di collegamento tra i dati trattati e gli USA; il controller era situato in Europa le banche dati erano, anch'esse, in Europa. In particolare il Garante esprimeva preoccupazione per quanto riguarda i trasferimenti di dati in massa in quanto il ricorso ad essi non è certamente limitato e può svilupparsi in una pratica comune. La definizione dello scopo per il quale i dati vengono trasferiti era più ampia di quella dell'art. 1 della Decisione Quadro del Consiglio 2002/475/JHA sulla lotta al Terrorismo. La conservazione di dati per 5 anni non è sostenuta dalla prova che questo periodo sia proporzionato. Inoltre l'accordo non specificava per quanto tempo i dati dovessero essere immagazzinati.

In definitiva il Garante Europeo opinava che non sufficienti elementi fossero stati forniti al fine di giustificare la necessità e la proporzionalità di tale accordo altamente invasivo per la privacy che in molti aspetti confligge con altri strumenti europei ed internazionali in tale area. Inoltre, alcuni elementi dell'accordo non sono definiti in maniera sufficientemente chiara da rendere prevedibile per gli europei i cui dati vengono trasferiti gli USA lasciando permanere diverse pericolose lacune che dovrebbero essere analizzate sotto la prospettiva dell'art. 1 TFUE ed il nuovo quadro normativo introdotto dal Trattato di Lisbona.

In data 11 febbraio 2010, la sessione plenaria del Parlamento respinse l'accordo TFTP. La principale motivazione del rigetto concerneva il trasferimento di blocchi di dati al Dipartimento del Tesoro. Inoltre i membri del parlamento avevano richiesto ulteriori stipule quali reciprocità nell'accesso alle informazioni di cittadini USA ove l'Unione Europea dovesse decidere di creare un simile TFTP, più stringenti limitazioni sull'immagazzinamento dei dati, rimedi per i cittadini

[381] Idem
[382] Corte Edu, sentenza sul ricorso n° 28341/95 del 4 maggio 2000, Rotaru c/ Romania
[383] André PRÜM nota 373

europei ove i dati vengano utilizzati per fini non consentiti e la possibilità di rescindere l'accordo in caso di prove di violazioni della privacy.

4. La rinegoziazione di un nuovo accordo. L'approvazione del TFTP II da parte del Parlamento Europeo.

La decisione di rigetto dell'accordo *ad interim* da parte del Parlamento Europeo ha avuto come effetto immediato quello di rinviare nuovamente gli Stati Uniti e l'Unione Europea ai tavoli del negoziato.

Infatti, la motivazione della decisione negativa del Parlamento muoveva essenzialmente dal presupposto che l'accordo, così come confezionato, offriva una scarsa protezione dei dati personali oggetto del trasferimento, soprattutto avuto riguardo alla previsione di trasferimenti in massa di dati (che secondo il Parlamento non potevano essere ammessi) ed all'assenza di qualsiasi forma di controllo, da parte di un'autorità giudiziaria indipendente, sulla legittimità delle richieste di trasmissione avanzate dal Dipartimento del Tesoro americano[384].

Ciò premesso, a seguito del veto opposto dal Parlamento, la Commissione pubblicava, in data 15 giugno 2010, una nuova proposta di decisione relativa alla conclusione di un nuovo accordo, ribattezzato "TFTP II". Tale proposta, oltre a contenere i frutti dei rinnovati negoziati con gli Stati Uniti recepiva, altresì ,alcune delle indicazioni del Parlamento Europeo, ed era diretta a dare una risposta alle preoccupazioni relative alla protezione dei dati personali.

In particolar modo, secondo il testo della proposta, la validità e la legittimità delle richieste di trasferimento avanzate dagli USA sarebbero state valutate da Europol. Inoltre, si sarebbe prevista una forma di controllo da parte dell'Unione Europea sul TFTP in territorio americano e la creazione, in un vicino futuro, di un programma europeo equivalente al TFTP, in modo tale da superare la necessità stessa di un accordo *ad hoc* con gli Stati Uniti. I cittadini europei avrebbero, poi, ottenuto gli stessi diritti dei cittadini americani ai sensi del *Privacy Act* al fine di azionare, innanzi ai competenti tribunali statunitensi, eventuali azioni a tutela dei propri dati personali nell'ambito del TFTP.

Il Garante Europeo per la Protezione dei Dati, a cui era stato chiesto di esprimere un parere consultivo sulla proposta di decisione relativa alla conclusione dell'accordo TFTP II[385], constatava

[384] Rob Turner "*European Parliament Rejects SWIFT deal for sharing bank data with the US*" reperibile su http://www.dw.de/european-parliament-rejects-swift-deal-for-sharing-bank-data-with-us/a-5239595-1 aggiornato al 4.10.2012

[385] Cfr. *Parere del GEPD sulla proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra l'Unione Europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione*

come il progetto contenesse alcuni miglioramenti rispetto all'accordo interinale TFTP I, tra cui l'esclusione dei dati relativi allo spazio unico dei pagamento in euro e l'utilizzo di una definizione di terrorismo più vicina a quella europea, un quanto ricalcata secondo l'approccio di cui all'art. 1 della decisione quadro 2002/475/GAI del Consiglio[386].

Inoltre, in tale sede, il GEPD coglieva l'occasione per ribadire la necessità di pervenire ad un accordo generale con gli Stati Uniti in merito alla protezione dei dati personali nel quadro della cooperazione di polizia e giudiziaria in materia penale che andasse a sostituire, tra l'altro, anche gli accordi *ad hoc* già vigenti (PNR e TFTP appunto)[387].

Ciò premesso, tra le osservazioni presentate dal Garante Europeo per la Protezione dei Dati vi erano altresì, alcune critiche, tra cui, anzitutto la mancata indicazione, nel testo della proposta, dell'art. 16 TFUE quale base giuridica per la conclusione dell'accordo TFTP II. In particolare, osservava il GEPD, poiché l'accordo si riferiva non soltanto allo scambio ma anche alla protezione dei dati personali, l'art. 16 TFUE costituiva una base giuridica non meno importante di quanto non lo fossero agli articoli 92 e 97 del TFUE che riguardavano la cooperazione giudiziaria[388]. Allo stesso modo, il GEPD esprimeva le sue perplessità con riguardo alla reale necessità di concludere un accordo specifico in materia di trasferimento dei dati di messaggistica finanziaria, vista l'esistenza di un accordo relativo alla mutua assistenza giudiziaria tra l'UE e gli USA che già autorizzava esplicitamente lo scambio di informazioni sui conti bancari e sulle transazioni finanziarie tra le autorità di contrasto, senza poi contare gli ulteriori strumenti di cooperazione già esistenti tra USA Europol ed Eurojust[389].

Quanto al principio di proporzionalità, il GEPD osservava come, malgrado le richieste del Parlamento Europeo, la nuova proposta continuasse a prevedere il trasferimento in massa di dati[390]. In quest'ottica, secondo il GEPD, la evidente difficoltà ad effettuare delle richieste mirate nel campo della messaggistica finanziaria, non poteva essere considerata motivo sufficiente per legittimare siffatti trasferimenti di massa, dovendosi al contrario individuare degli strumenti idonei al fine di assicurare l'invio esclusivo di dati pertinenti e necessari alle richieste statunitensi. Allo stesso modo, il GEPD osservava come il periodo di conservazione previsto di 5 anni con riferimento ai dati non estratti avrebbe dovuto essere molto inferiore, specie con riferimento a quei

---

Europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II) in GUUE 2010/C/ 355/02 del 29.12.2010.

[386] Decisione Quadro del Consiglio 2002, del 13 giugno 2002 sulla lotta contro il terrorismo, (GU L 164 del 22.06.2002, pag. 3)

[387] Cfr. punti 7 e 8 del Parere del GEPD cit sub nota 52.

[388] Cfr. punto 5 del Parere del GEPD cit sub nota 52

[389] Cfr. punti 14-17 del Parere del GEPD cit sub nota 52

[390] Cfr. punto 18 del Parere del GEPD cit sub nota 52

dati che non venivano specificamente consultati né utilizzati per un'indagine o un'azione penale specifica[391].

Ferme restando le suesposte considerazioni, inoltre, il GEPD rilevava come, sebbene la proposta di decisione avesse previsto un meccanismo di trasferimento dei dati basato su un sistema *push* anziché *pull*, essa non disciplinasse alcuna forma di controllo, da parte di un'autorità giudiziaria pubblica, della legittimità delle richieste di trasferimento inoltrate dal Dipartimento del Tesoro, ma si limitava a conferire tale compito a Europol, agenzia UE istituita per prevenire e combattere la criminalità organizzata, il terrorismo e altre gravi forme di criminalità che interessano due o più stati membri[392]. In particolare, secondo il GEPD, l'Agenzia "Europol", oltre a non essere un'autorità giudiziaria, presentava interessi specifici ad ottenere i dati personali oggetto di trasferimento, elemento che avrebbe potuto pregiudicarne l'indipendenza nell'esercizio delle designate funzioni di supervisore, senza tenere poi conto del fatto che la missione istituzionale dell'agenzia esigeva pur sempre il mantenimento di buone relazioni con il dipartimento del Tesoro statunitense. Inoltre, sulla base del quadro giuridico post Lisbona non era chiaro se una decisione Europol adottata nei confronti di una società privata potesse essere soggetta a controllo giudiziario da parte della Corte di Giustizia dell'Unione Europea. Sulla base di tali considerazioni il GEPD tornava dunque a richiedere che il compito di valutare le richieste del Dipartimento del Tesoro Statunitense venisse affidato ad un'autorità giudiziaria pubblica.

Analoghe perplessità venivano espresse dal GEPD con riguardo al sistema di rimedi offerti ai cittadini europei secondo la nuova proposta. Infatti, sebbene gli Stati Uniti in sede di negoziato avessero acconsentito ad estendere ai cittadini europei la protezione di cui al Privacy Act, il GEPD osservava come tale legge stabilisse chiaramente che una richiesta di accesso ai propri dati personali era formulabile soltanto da parte di un cittadino statunitense stabilmente e legalmente residente negli USA[393]. Pertanto il GEPD raccomandava di rivedere la formulazione della proposta al fine di garantire che i diritti da essa garantiti fossero realmente azionabili da parte dei cittadini europei in territorio statunitense.

Infine il GEPD auspicava un miglioramento dei meccanismi di supervisione e di controllo previsti dalla proposta al fine di far si che i compiti e il ruolo della personalità nominata dalla Commissione europea e di rappresentanti delle autorità europee di protezione dei dati fossero ben definite e che tali figure fossero messe in condizioni tali da poter agire in modo indipendente e di adempiere in maniera efficace ai propri compiti di supervisione. In tal senso il GEPD sottolineava

[391] Cfr. punti 21 e 22 del Parere del GEPD cit sub nota 52.
[392] Cfr. punti 23 e 24 del Parere del GEPD cit sub nota 52
[393] Tale disposizione trovava conferma nell'informativa disponibile sul sito internet del dipartimento del Tesoro Statunitense al sito http://www.treas.gov/foia/how-to.html a far data al 21.06.2010

come la supervisione indipendente costituisse un elemento chiave del diritto alla protezione dei dati personali come confermato, oltre che dalla legislazione vigente anche dalla recente sentenza del 9 marzo 2010 Commissione c. Germania[394] nel cui ambito la Corte di Giustizia ha stabilito dei rigidi criteri per l'indipendenza.

Ciò premesso, in data 8 luglio 2010 il Parlamento Europeo approvava il nuovo accordo TFTP II con 484 voti a favore, 109 contrari e 12 astensioni, consentendone l'entrata in vigore il 1 Agosto 2010. Cinque giorni dopo, in data 13 luglio 2010 il Consiglio Approvava definitivamente l'accordo.

La versione definitiva dell'accordo contiene le seguenti disposizioni salienti.

Innanzitutto le informazioni ricavabili dai messaggi finanziari che vengono immagazzinati nel territorio della UE dai fornitori di servizi di comunicazione finanziaria potranno essere fornite al Dipartimento del Tesoro americano su sua richiesta per le sole finalità di prevenzione, indagine o repressione del terrorismo e del finanziamento del terrorismo (art. 1 e 3). A differenza di quanto previsto dall'accordo TFTP I, la definizione di terrorismo nell'accordo vigente ricalca quella di cui alla decisione quadro 2002/475/GAI del Consiglio.

Viene poi specificato che le richieste del Dipartimento del Tesoro dovranno identificare nella maniera più precisa possibile i dati oggetto delle stesse e sostanziarne la necessità nella maniera più univoca possibile[395]. L'art. 4 dell'Accordo, nonostante i rilievi mossi dal Parlamento e le osservazioni sviluppate dal GEPD, prevede comunque l'attribuzione ad Europol, e non ad un'autorità giudiziaria pubblica, del compito di verificare che le richieste del Dipartimento del Tesoro rispondano ai requisiti dell'accordo.

Viene inoltre previsto (art. 5 par. 3) l'impegno da parte dell autorità statunitensi di astenersi da qualsiasi attività *di data mining* o da qualsiasi altro tipo di *profiling* automatizzato o algoritmico o di *computer filtering* sui dati ricevuti. L'art- 5 specifica poi le garanzie quanto alla sicurezza ed all'integrità dei dati raccolti, in particolare i dati dovranno essere immagazzinati in un ambiente sicuro, separato da altri dati e non interconnesso con altre banche dati. Viene poi previsto che tutte le ricerche dovranno essere basate su informazioni pre-esistenti o prove che dimostrino una ragione di credere che il soggetto della ricerca abbia un legame con il terrorismo o il suo finanziamento.

L'accordo prevede, inoltre, all'art. 6 un sistema di revisione annuale da parte del Dipartimento del Tesoro volto ad individuare dati non estratti che non siano più necessari alla lotta contro il terrorismo. In tal caso questi dati dovranno essere eliminati permanentemente. Allo stesso modo tutti i dati ricevuti prima del 20 luglio 2007 dovranno essere cancellati entro il 20 luglio 2012.

[394] Causa C-518/07 Commissione c. Germania, sentenza del 9 marzo 2010

[395] Marie-Élisabeth MATHIEU "*Entrée en vigueur le 1er août 2010*" Revue de Droit bancaire et financier n° 5, Septembre 2010, comm. 183

L'accordo è soggetto a revisione congiunta da parte delle Parti Contraenti contraenti, al fine di rivedere le garanzie i controlli e le disposizioni di reciprocità. Tali revisioni vengono stabilite di comune accordo.

Infine l'art. 21 autorizza ciascuna parte contraente a sospendere l'accordo con effetti immediati in caso di violazione da parte dell'altra parte contraente. Allo stesso modo è prevista la possibilità di porre termine all'accordo anticipatamente e indifferentemente dall'inadempimento della controparte con decorrenza di sei mesi dalla data di notifica attraverso i canali diplomatici.

Secondo parte della dottrina[396], il testo finale dell'accordo non sembra venire troppo incontro alle preoccupazioni espresse dal Parlamento Europeo in sede di rigetto della sua prima versione. A ben vedere, infatti, i cambiamenti cruciali richiesti dal Parlamento non sono stati apportati, mentre le altre modifiche si palesano come meramente marginali.

In particolare, parte della dottrina ha evidenziato come il trasferimento in massa di dati venga consentito anche nella versione definitiva dell'accordo, il che potrebbe significare che i nomi di milioni di persone possano finire sulle liste dei terroristi anche senza particolari prove. Inoltre, viene criticato l'art. 6 che consente agli USA di trattenere i dati, sostanzialmente per un tempo indeterminato[397].

Allo stesso modo, è stato rilevato come l'accordo TFTP II permetta di seguire le attività finanziarie tanto delle società (che hanno il maggior numero di movimenti) che degli individui. Grande è il rischio che i trasferimenti in blocco di dati possano essere usati per spionaggio industriale sulle transazioni finanziarie delle aziende europee[398].

La dottrina ha, poi, stigmatizzato il mancato accoglimento della richiesta del Parlamento Europeo di sottoporre il trasferimento dei dati ad una autorità giudiziaria indipendente. Infatti, EUROPOL non è un'autorità indipendente, bensì un'emanazione della polizia degli stati membri, che vanta uno specifico interesse ad ottenere i dati per sé stessa.

In buona sostanza, parte della dottrina ha criticato l'atteggiamento dell'Unione Europea, sottolineando come la stessa avrebbe firmato un assegno in bianco alle autorità degli Stati Uniti, accordo che finisce col colpire indistintamente tutti i cittadini senza ragioni specifiche. Invero, gli individui sono in una posizione di sostanziale impotenza in quanto i loro dati vengono condivisi e trattati a loro insaputa e senza il loro consenso da parte di poteri indipendenti[399].

[396] Sylvia Kierkegaard, nota 375
[397] Idem
[398] Ibidem
[399] Sylvia Kierkegaard, nota 375

In conclusione la vicenda SWIFT costituisce uno degli esempi più eclatanti dello scontro culturale e normativo che interessa i rapporti tra Unione Europea e Stati Uniti in materia di tutela dei dati personali.

Infatti, parte della dottrina americana ha interpretato la vicenda SWIFT come un arrogante tentativo, da parte dell'Unione Europea, di imporre ai suoi alleati dei principi di diritto, in materia di tutela dei dati, che sono il frutto di esperienze storiche e tradizioni normative che non sono condivise universalmente[400]. Allo stesso modo, la vicenda SWIFT ha posto in risalto quelle che sarebbero delle vere e proprie *defaillances* della Direttiva 95/46/CE, che risulta in tal modo essere uno strumento normativo antiquato, incapace di fare fronte alle nuove esigenze derivanti dalla lotta al terrorismo.

Secondo parte della dottrina europea, al contrario, la vicenda SWIFT avrebbe posto in luce lo scarso spirito collaborativo degli Stati Uniti nei confronti dei propri alleati. Invero, all'epoca della vicenda SWIFT esistevano, a livello internazionale, degli efficaci sistemi di cooperazione e di lotta al terrorismo che potevano essere messi in pratica nel rispetto della sovranità nazionale dei paesi aderenti. Secondo parte della dottrina gli Stati Uniti avrebbero potuto, dunque, fare ricorso a tali sistemi di cooperazione piuttosto che agire unilateralmente nei confronti di una società europea senza informarne le autorità europee competenti[401].

In data 25 giugno 2003, inoltre, Stati Uniti e Unione Europea avevano firmato un accordo internazionale sulla mutua assistenza legale e l'estradizione. Sebbene questi trattati non fossero stati ancora ratificati all'epoca della vicenda Swift, l'art. 18 della Convenzione di Vienna sul diritto dei Trattati afferma che uno Stato è obbligato ad astenersi dal compiere atti che possano frustrare l'oggetto e lo scopo del trattato allorquando abbia firmato il trattato o abbia scambiato strumenti costituenti il trattato soggetto a ratifica, purché non abbia notificato l'intenzione di non divenire parte al trattato stesso. Gli Stati Uniti avrebbero, quindi, dovuto ricercare comunque la collaborazione delle autorità europee anziché procedere unilateralmente.

Invero, buona parte della dottrina europea resta ancorata all'idea che la lotta contro il terrorismo non dovrebbe essere mai usata come scusa per limitare i diritti fondamentali[402]. Allo stesso modo, e chi scrive si sente di condividere, è semmai compito della giustizia penale e non certo dei servizi di informazione, quello di tutelare le libertà e la sicurezza dei cittadini nei confronti del terrorismo.

[400] Santolli Justin, nota 287.
[401] E. Caprioli, " *Violation des règles propres aux données à caractère personnel et réseau SWIFT*", in Revue de Droit bancaire et financier n° 1, Janvier 2007, 34
[402] Sylvia Kierkegaard, nota 373

PARTE TERZA
IL CONTENZIOSO USA-UE NELL'AMBITO DELLA VICENDA PNR

1. Terrorismo internazionale ed evoluzione delle misure di sicurezza aeree negli Stati Uniti d'America.

A partire dal 1968, anno del dirottamento del volo *El Al 426 Roma-Tel Aviv*, gli attentati aerei motivati da ragioni politiche o da finalità di terrorismo sono diventati un pericolo concreto ed attuale per l'aviazione civile. In risposta a questa minaccia, sono stati introdotti ovunque nel mondo controlli sui bagagli e sui passeggeri[403].

Negli Stati Uniti d'America, la tragica esplosione del Boeing 747-131 della *Trans World Airlines* nel 1996[404], la cui dinamica poco chiara costò la vita a 230 persone, indusse l'amministrazione Clinton ad introdurre, sulla base delle raccomandazioni formulate dalla *Aviation Security Commission*, un sistema computerizzato di controllo dei passeggeri, il *Computer Assisted Passenger Pre-screening System* (in prosieguo "CAPPS") [405].

Detto sistema, entrato in funzione nel 1999, aveva come scopo quello di elaborare i dati estrapolati dai *passenger name record* delle compagnie aeree al fine di individuare automaticamente i soggetti che potevano presentare rischi per la sicurezza e sottoporli, così, a procedure di controllo più rigorose[406].

Notoriamente, i *passenger name record* (in prosieguo "PNR") consistono in un insieme di informazioni che vengono raccolte dalle compagnie in sede di prenotazione di un biglietto aereo. Tra le informazioni raccolte rientrano anche quei dati che non sono strettamente necessari alla transazione, ma il cui trattamento è comunque finalizzato a fornire un migliore servizio alla clientela.

Poche compagnie americane gestiscono autonomamente le proprie banche dati PNR; molti di questi dati vengono perlopiù raccolti in uno dei quattro principali *Computer Reservations Systems* (in prosieguo "CRS"), ove le informazioni vengono conservate a tempo indeterminato[407]. I PNR generalmente contengono:

---

[403] Bruce Hoffmann, "*Inside Terrorism*", New York 1998, p. 67

[404] CNN, *"Six months later still no answer to TWA Flight 800 mistery"*, consultabile su http://edition.cnn.com/US/9701/17/twa/index.html aggiornato al 20.05.2010

[405] CNN, *"Clinton signs airport security measures into law",* consultabile su http://edition.cnn.com/US/9610/09/faa/index.html aggiornato al 20.05.2010

[406] Ioannis Ntouvas, *"Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments",* in International Journal of Law & Information Technology, 16 n.1 73-95, 2008.

[407] D. Richard Rasmussen *"Is international travel per se suspicion of terrorism? The dispute between the United States and European Union over passenger name record data transfers"* , 26 Wisconsin International Law Journal, 551, 2008

1. Nome e cognome
2. Indirizzo privato e/o lavorativo
3. Numero di telefono cellulare e fisso
4. Indirizzo di posta elettronica
5. Il nome e le informazioni di contatto per le chiamate di emergenza
6. Dettagli di viaggio, incluse informazioni di volo, prenotazioni di hotel, noleggio di autoveicoli, crociere ed altri servizi di viaggio
7. Dettagli di pagamento e informazioni sulla carta di credito
8. Qualsiasi informazione aggiuntiva, quale eventuali problemi di salute associati al volo, invalidità o preferenze alimentari ispirate da motivi religiosi[408].

I PNR possono, inoltre, includere informazioni relative a persone che non prendono mai l'aereo. Molte agenzie di viaggio, infatti, incluse quelle *online*, registrano presso un CRS le informazioni riguardanti prenotazioni di alberghi, noleggio di autoveicoli ed altri servizi di viaggio anche qualora non siano stati acquistati dei biglietti aerei. Allo stesso modo, i CRS conservano una cronologia relativa a ciascun passeggero che comprende tutti i dati PNR raccolti dalle compagnie aeree, le informazioni "*frequent flyer*" e la fonte di provenienza di qualsiasi prenotazione o richiesta speciale, incluse le informazioni di contatto degli agenti di viaggio[409].

Nei CRS vengono, altresì, registrate le informazioni relative a gruppi di persone, familiari o colleghi di lavoro che hanno viaggiato col passeggero. Anche se una prenotazione può essere, dunque, disdetta e i relativi dati PNR cancellati, presso il CRS verrà comunque conservata a tempo indeterminato tutta la cronologia delle transazioni effettuate.

Il CRS, inoltre, crea un profilo per ciascun cliente regolare, incluso un aggregato delle informazioni ricavabili da tutti i PNR, ed evidenzia le preferenze del passeggero in virtù delle sue richieste passate. Questo profilo non è finalizzato alla vendita dei biglietti da parte delle compagnie aeree ma viene utilizzato dagli intermediari turistici per scopi commerciali e dalle autorità di pubblica sicurezza per finalità di controllo dell'immigrazione[410].

E' facile comprendere, pertanto, come queste informazioni, oltre a risultare particolarmente utili per le finalità di lotta al terrorismo, si caratterizzino spesso anche per il loro carattere sensibile. Si pensi, infatti, ai dati relativi allo stato di salute dei passeggeri ovvero alle abitudini alimentari ispirate da un particolare credo religioso.

---

[408] Edward Hasbrouck *"What's in a Passenger Name Record (PNR)?",* consultabile su http://hasbrouck.org/articles/PNR.html aggiornato al 20.05.2010.
[409] *Idem*
[410] Ibidem

Nello specifico il CAPPS serviva, appunto, ad elaborare i dati estrapolabili dai PNR attraverso la loro comparazione con le informazioni contenute in liste governative di nomi di persone sospettate di terrorismo. Inoltre, tale sistema effettuava l'analisi delle caratteristiche comportamentali dei passeggeri. Ciò serviva, in particolare, ad evidenziare eventuali casi di comportamento di viaggio sospetto a loro volta deducibili da elementi quali modalità di pagamento anomale o durata singolare del viaggio[411].

Il CAPPS suddivideva, quindi, i passeggeri in due gruppi separando quelli per i quali era sufficiente un controllo di tipo generale da quelli che, invece, necessitavano di uno *screening* più approfondito o nei cui confronti vigeva un divieto assoluto di imbarco. Il tutto con lo scopo di aumentare la sicurezza aeroportuale, senza generare eccessivi ritardi per i passeggeri[412].

Il sistema CAPPS, tuttavia, divenne ben presto bersaglio di critiche da parte dell'opinione pubblica in ragione dei potenziali rischi per i diritti fondamentali e per la privacy. Soltanto un anno dopo la sua istituzione, infatti, il CAPPS venne limitato al controllo bagagli dei passeggeri[413].

L'attentato dell'11 settembre 2001, in cui il dirottamento di quattro aerei di linea venne per la prima volta utilizzato come arma contro obiettivi civili, ha portato ad un ripensamento del CAPPS, accusato anzi di non essere stato insufficiente a scongiurare la tragedia, nonché all'emanazione di norme di controllo più stringenti in materia di sicurezza dei voli di linea, attraverso l'approvazione *dell'Aviation and Transportation Security Act* (in prosieguo "ATSA")[414].

L'emanazione dell'ATSA da parte del Congresso ha comportato un radicale cambiamento nella modalità di gestione della sicurezza aerea negli Stati Uniti. In epoca precedente agli attentati di New York e di Washington, infatti, tutte le questioni relative alla sicurezza dell'aviazione civile erano demandate alla *Federal Aviation Administration* (in prosieguo "FAA"), un'agenzia governativa alla quale era stato attribuito, mediante il *Federal Aviation Act*, il compito di stabilire linee guida, regolamenti e decisioni concernenti l'industria dei trasporti aerei.

In particolare, la FAA, nell'esercizio delle sue competenze, aveva provveduto a trasferire la responsabilità per la sicurezza dei voli alle stesse compagnie aeree. Tuttavia, queste ultime,

[411] James Fisher in *"What price does society have to pay for security? A look at the aviation watch list"* in 44 Willamette Law Review, 2008
[412] Idem
[413] Ibidem
[414] *Aviation and Transportation Security Act*, *Public Law 107-71* del 19 novembre 2001

sulla base della logica del contenimento dei costi, si erano rivolte ad entità private, alle quali era stato in definitiva affidato il compito di gestire le operazioni di controllo negli aeroporti[415].

L'attuazione della nuova normativa ha comportato il sovvertimento di tale impostazione, grazie alla federalizzazione della sicurezza aeroportuale a sua volta ottenuta mediante l'istituzione della *Transportation Security Administration* (in prosieguo "TSA") presso il *Department of Homeland Security* (in prosieguo "DHS").

Tale agenzia amministrativa riceveva mandato dal Congresso per la gestione della sicurezza dell'aviazione civile, che veniva così sottratta alle compagnie aeree, nonché per la progettazione e la sperimentazione del cd. "CAPPS II", destinato a sua volta a diventare l'odierno "*Secure Flight Program*" [416].

I vantaggi del CAPPS II rispetto alla sua precedente versione derivavano essenzialmente dal fatto che la gestione ed il controllo erano oramai passate al governo federale. Il tutto nell'ottica di garantire al sistema un più efficace accesso alle informazioni di intelligence e di rendere CAPPS II maggiormente capace di adeguarsi al mutare costante delle minacce terroristiche.

Al pari della sua versione originaria, il CAPPS II era pensato per permettere alla TSA di acquisire i dati PNR, incluso indirizzo, data di nascita numero di telefono ed altre informazioni di viaggio dei passeggeri. Tuttavia, mentre il precedente sistema utilizzava i dati PNR al solo scopo di selezionare i passeggeri onde sottoporre il loro bagaglio ad uno *screening* più approfondito, il CAPPS II avrebbe utilizzato i PNR anche al fine di individuare i soggetti da sottoporre ad interrogatorio o perquisizione[417].

Sulla base dei dati PNR, inoltre, il nuovo sistema avrebbe effettuato delle valutazioni di sicurezza mediante controlli incrociati con le informazioni contenute nelle banche dati governative ed avrebbe, quindi, inoltrato il suo responso direttamente al banco del *check-in*: ai passeggeri di "rischio accettabile" sarebbe stato permesso di imbarcare direttamente, mentre quelli di rischio "sconosciuto" sarebbero stati controllati più rigorosamente. Quelli di "rischio inaccettabile", invece, sarebbero stati controllati direttamente dalla polizia[418].

Nel 2004, tuttavia, anche il sistema CAPPS II venne abbandonato in ragione delle critiche da parte dell'opinione pubblica[419] e delle forza politiche di opposizione.

---

[415] *Idem* sub 8 *supra*
[416] Irfan Tukdi "*Transatlantic Turbulence: The Passenger Name Record Conflict"* in *"Thirty years of airline deregulation : a structure, conduct and performance review"* , 45 Houston Law Review 587, 2008
[417] Idem
[418] Ibidem
[419] James Fisher, nota 411

Successivamente, il 9 agosto 2007 la TSA annunciava una proposta di regolamento volta ad istituire il programma *Secure Flight*[420]. Il *Secure Flight* è noto per essere un sistema automatico la cui funzione è sempre quella di prevenire che terroristi noti o sospetti possano imbarcare sugli aerei ove potrebbero mettere in pericolo la vita di passeggeri e di terzi, ovvero accedere alle aree cd. sterili degli aeroporti, cioè quelle destinate all'imbarco e che vengono controllate da personale della TSA.

Secondo fonti ufficiali, il nuovo sistema subiva dei miglioramenti che, a differenza dei sistemi di controllo precedenti, avrebbero dovuto limitarne l'utilizzo al contrasto del terrorismo anziché ad altri obiettivi di polizia giudiziaria[421].Il progetto non fu mai portato a termine a causa dell'opposizione del congresso americano[422].

Attualmente, dunque, ai sensi dell'*Aviation and Trasportation Security Act* tutte le compagnie aeree che viaggiano verso o dagli Stati Uniti, o che vi transitano sono tenute a fornire alle autorità doganali americane (*U.S. Commissioner of Customs*) due tipi di dati riferibili ai passeggeri: il manifesto dei passeggeri e dell'equipaggio[423], vale a dire le informazioni relative alle compagnie, ai voli, all'identità e all'itinerario di viaggio di tutti i passeggeri nonché i dati dei PNR.

La normativa americana prevede che il manifesto debba essere inoltrato direttamente al U.*S. Commissioner of Customs* a cura della compagnia aerea, mentre le autorità doganali statunitensi possono avere accesso diretto ai dati contenuti nei PNR. Tali informazioni devono, comunque, essere messe a disposizione non oltre quindici minuti prima del decollo dell'aereo in rotta verso gli USA[424].

I dati ricavati dai manifesti dei passeggeri vengono, quindi, elaborati direttamente dall'Amministrazione per la Sicurezza dei Trasporti e gestiti mediante gli "*Aviation Security Screening Records"*. Al fine di prevenire vari rischi per la sicurezza, incluso il terrorismo, questi dati vengono distribuiti a varie autorità ed entità private, e vengono conservate per un considerevole lasso di tempo (cinquant'anni). Il rapporto tra *Aviation Security Screening Records* e CAPPS è tutt'altro che chiaro[425].

---

[420] U.S. Department of Homeland Security, "*Privacy Impact Assessment for the Secure Flight Program*", August 9th 2007, consultabile su http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_secureflight.pdf aggiornato al 20 maggio 2010.

[421] James Fisher, nota 411

[422] http://www.gao.gov/new.items/d04385.pdf

[423] Nel linguaggio dei trasporti marittimi ed aerei il manifesto indica un prospetto particolareggiato del carico di una nave, firmato dal suo capitano e destinato ai funzionari della dogana.

[424] Christopher Patton, "*No man's land: the EU-US passenger name record agreement and what it means for the European Union's pillar structure*", in 40 George Washington International Law Review 527, 2008.

[425] Idem

La Sezione 115 *dell'Aviation and Transportation Security Act* non precisa le modalità di trasferimento dei dati. Tuttavia, il regolamento di attuazione stabilisce un sistema "*pull*". In particolare il metodo pull si basa sull'accesso diretto da parte del DHS agli archivi elettronici dei vettori aerei in cui vengono conservati tutti i dati relativi ai passeggeri. In questo caso le compagnie aeree europee devono limitarsi a consentire al DHS di entrare nei propri database senza restrizioni. Il metodo push, viceversa, comporta che siano i vettori aerei a trasferire alle competenti autorità USA i soli dati PNR espressamente previsti, eventualmente omettendo informazioni personali non pertinenti. Inoltre, l'ATSA prevede disposizioni sulla revoca dei privilegi di atterraggio o rigide sanzioni economiche a carico delle compagnie che rifiutano di rendere disponibili tali informazioni.

Le compagnie aeree europee, dunque, per le quali l'importanza di evitare le multe e di conservare remunerativi privilegi di atterraggio superavano per importanza qualsiasi questione relative alla privacy, si erano venute a trovare tra l'incudine della nuova normativa americana - che imponeva il trasferimento dei dati alle autorità doganali statunitensi - ed il martello della legislazione degli Stati membri dell'Unione Europea in materia di protezione dei dati personali –che invece lo vietava -[426] . Tale legislazione, infatti, di derivazione comunitaria, trova la propria genesi nella Direttiva 95/46/CE in materia di protezione dei dati personali, la quale vieta il trasferimento verso paesi terzi qualora questi ultimi non garantiscano un livello adeguato di protezione.

La vicenda dei PNR, che rappresenta tutt'oggi una delle maggiori operazioni di trasferimento di dati personali dall'Unione Europea agli Stati Uniti, ha generato ampie preoccupazioni in seno all'opinione pubblica europea per le sue implicazioni nel campo della privacy ed ha indotto la Commissione ad instaurare dei negoziati con le autorità americane al fine di pervenire allo sblocco della situazione ora descritta.

In prosieguo verranno descritti i frutti dei negoziati e l'impatto che la vicenda PNR ha avuto sulla dimensione esterna della protezione dei dati personali in Europa.

2. La genesi dell'accordo PNR

Come si è visto nelle pagine che precedono, a seguito degli attacchi terroristici dell'11 settembre 2001, gli Stati Uniti hanno adottato una normativa che imponeva a tutti vettori aerei assicuranti collegamenti aventi come partenza, destinazione o transito il territorio americano di fornire alle autorità doganali statunitensi l'accesso diretto ai dati contenuti nel loro sistema

[426] Ibidem

automatico di prenotazione e di controllo delle partenze, denominati «Passenger Name Records» (in prosieguo: i «dati PNR»).

Le compagnie aeree di quasi tutti paesi del mondo si piegarono spontaneamente alle richieste del governo americano e ciò in ossequio a diverse ragioni.

Innanzitutto, già da prima degli attentati del 2001, diverse compagnie aeree fornivano volontariamente alle autorità americane parte dei loro dati PNR. In secondo luogo, a seguito degli attentati alle torri gemelle, diversi altri paesi oltre agli USA (si pensi all'Australia e all'Inghilterra, al Canada e alla Nuova Zelanda) iniziarono ad introdurre nei propri aeroporti dei sistemi di controllo simili al CAPPS[427]. Infine, la nuova legislazione americana avrebbe comportato, in caso di mancata spontanea comunicazione dei dati PNR alla Customs and Border Protection (in seguito "CBP"), l'irrogazione di pesanti sanzioni oltre che il rischio concreto, per le compagnie inadempienti, di vedersi togliere i diritti di atterraggio sul suolo americano.

La situazione appena descritta poneva, tuttavia, le compagnie aeree europee soggette alla direttiva 95/46/CE in materia di protezione dei dati personali, in una condizione di grave difficoltà sotto il profilo giuridico. Invero, il trattamento dei dati PNR da parte delle compagnie costituiva un'operazione soggetta alla Direttiva in quanto riguardava dati riferibili a persone fisiche che erano stati raccolti a fini commerciali. Inoltre, sempre a norma delle disposizioni della direttiva medesima, la comunicazione dei dati PNR alle autorità doganali americane configurava un trasferimento di dati personali verso uno Stato terzo, ovvero gli USA, che non assicurava un livello adeguato di protezione di tali dati. Detto trasferimento, pertanto, risultava vietato ai sensi della Direttiva 95/46 sulla protezione dei dati personali.

Per queste ragioni le stesse compagnie aeree, in caso di ottemperanza alle richieste americane, sarebbero state passibili di sanzioni da parte delle autorità garanti dei paesi europei per violazione delle legislazioni nazionali di attuazione della direttiva 95/46/CE.

La situazione appena descritta si pone, così, all'origine della controversia internazionale tra Stati Uniti e Unione Europea in merito al trasferimento dei dati dei dossier PNR.

Sin dal giugno 2002 la Commissione Europea, pur riconoscendo la legittimità degli interessi di sicurezza in gioco, informava le autorità statunitensi del fatto che le nuove disposizioni in materia di trasferimento dei dati PNR rischiavano di entrare in contrasto con la legislazione comunitaria e con quella degli Stati membri in materia di tutela dei dati[428], nonché con talune disposizioni del regolamento (CEE) del Consiglio 24 luglio 1989, n. 2299, relativo ad un codice di comportamento

[427] Christopher Patton, nota 424

[428] Comunicazione della Commissione al Consiglio e al Parlamento sul Trasferimento dei dati PNR aerei: "*A Global EU Approach*" disponibile su http://ec.europa.eu/justice/policies/privacy/docs/adequacy/apis-communication/apis_en.pdf

in materia di sistemi telematici di prenotazione[429] ,come modificato dal regolamento (CE) del Consiglio 8 febbraio 1999, n. 323[430].

Le autorità statunitensi rinviavano temporaneamente l'entrata in vigore delle nuove disposizioni, rifiutandosi però, in definitiva, di rinunciare ad infliggere sanzioni alle compagnie aeree che non si sarebbero conformate alla normativa sull'accesso elettronico ai dati PNR dopo il 5 marzo 2003[431].

Per questo motivo, nel febbraio 2003 la Commissione europea e la CBP emanarono una dichiarazione congiunta[432] in base alla quale la Commissione avrebbe autorizzato le compagnie aeree europee a trasferire i dati PNR al CBP. Alla dichiarazione veniva allegato un documento contenente determinati impegni («undertakings») assunti dal CBP[433], in vista dell'adozione da parte della Commissione, sulla base dell'art. 25, n. 6, della direttiva, di una decisione sull'adeguatezza. Tuttavia tale soluzione era temporanea in quanto vincolava all'impegno di intraprendere negoziazioni al fine di trovare una soluzione definitiva al problema. Da allora, in ogni caso, numerose grandi compagnie aeree dell'Unione europea presero a fornire alle autorità americane libero accesso ai propri dati PNR[434].

3. I Rilievi critici del Gruppo per la tutela delle persone fisiche con riguardo al trattamento dei dati personali (Gruppo ex. Art. 29)

Il 13 giugno 2003 il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della Direttiva, emanava un parere in cui esprimeva seri dubbi circa l'adeguatezza del livello di tutela dei dati garantito dagli undertakings del Governo USA[435]. Tali dubbi sono stati successivamente reiterati in un parere del 29 gennaio 2004[436].

In tali occasioni il Gruppo identificava una serie di aspetti problematici relativi alle richieste statunitensi e le ragioni per le quali queste ultime risultavano chiaramente in contrasto con i principi della direttiva 95/46/CE.

---

[429] Cfr. GUUE L 220, pag. 1
[430] Cfr. GUUE L 40, pag. 1
[431] Cfr. Nota 25 supra
[432] Joint statement approvato al termine della riunione tenutasi a Bruxelles il 17 e il 18 febbraio 2003 tra rappresentanti della Commissione europea e del CBP
[433] Undertakings of the Department of Homeland Security Bureau of Customs and Border Protection Regarding the Handling of Passenger Name Record Data, 69 Fed. Reg. 41543 (Jul. 9, 2004);
[434] Idem supra
[435] Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data reperibile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2003/wp78_en.pdf
[436] Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be transferred to the United States' Bureau of Customs and Border Protection (US CBP)Adopted on 29 January 2004 consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_en.pdf

Attesa l'elevata competenza del Gruppo ex art. 29 nel campo della tutela dei dati personali, nonché l'autorevolezza e la rilevanza del duplice intervento in questione, vale la pena di riassumerne in questa sede i contenuti principali.

Innanzitutto il Gruppo di Lavoro evidenziava come i dati richiesti dagli USA alle compagnie europee eccedessero quelli generalmente raccolti nell'esercizio dell'attività di impresa e come il trasferimento degli stessi non potesse essere considerato compatibile con lo scopo originario della loro raccolta da parte delle compagnie o delle agenzie di viaggio nell'ambito delle rispettive obbligazioni contrattuali[437]. Ciò configurava, dunque, oltre che una violazione del principio di limitazione dei dati, anche una violazione dell'art. 6 della Direttiva che codifica il principio della finalità del trattamento[438].

In secondo luogo, il trasferimento in questione non poteva giustificarsi alla luce di alcuna delle deroghe di cui all'art. 26 della Direttiva posto che queste ultime si caratterizzano per il loro carattere eccezionale laddove, invece, il trasferimento dei dati PNR alle autorità americane sarebbe avvenuto, in forma continuativa e sistematica[439]. Allo stesso modo, tale trasferimento di massa non avrebbe potuto avvenire nel quadro del programma "Safe Harbor", in quanto la condivisione dei dati PNR non avveniva per scopi commerciali, bensì per finalità di lotta al terrorismo ed alla criminalità organizzata[440].

Inoltre, il Gruppo di Lavoro metteva in evidenza come, sempre a seguito dell'irrigidimento della normativa USA in materia di sicurezza aerea, la lista dei dati oggetto di trasmissione fosse andata ampliandosi sempre di più[441].

Infine il Gruppo di Lavoro osservava come i dati trasmessi venissero inoltrati ad una banca dati centralizzata che veniva gestita sia dalla *US Customs and Border Protection* che *dalla US*

[437] Cfr. Opinion 4/2003 sub nota 33
[438] Idem
[439] Idem *ut supra*
[440] Ibidem
[441] Invero, le compagnie aeree avevano l'onere di inoltrare numerosi informazioni e partitamente: nome, cognome, data di nascita, nazionalità, sesso, numero di passaporto e luogo di emissione, paese di residenza, numero di visto USA, data e luogo di rilascio, numero di registrazione stranieri, indirizzo negli Stati Uniti durante la permanenza e qualsiasi informazione ritenuta necessaria al fine di identificare la persona che viaggia e proteggere la sicurezza nazionale. Quest'ultimo in particolare poteva contenere non soltanto informazioni relative ai voli passati ma anche informazioni etniche o religiose (scelta di un particolare menu *halal* o *kosher* ad esempio), l'affiliazione ad un determinato gruppo, dati relativi al luogo di residenza (indirizzo email, informazioni su amici, parenti, luogo di lavoro ecc.), dati medici(es. tipologia di assistenza medica richiesta, ossigeno, problemi di vista o mobilità che devono essere comunicati alla compagnia aerea) o altri dati connessi, quali le informazioni *frequent flier*. Inoltre, per i paesi (tra cui anche l'Italia) partecipanti al programma "Viaggio senza Visto", il trasferimento dei dati biometrici era divenuto obbligatorio a far data dal 2004. Inoltre, tra i dati richiesti figuravano,altresì, i Passenger Name Records (PNR) i quali includono, oltre ai dati identificativi del passeggero e al numero di telefono, anche il numero di prenotazione PNR, la data della prenotazione, l'agenzia di viaggio, le informazioni figuranti sul biglietto, le informazioni relative alla carta di credito (numero di carta di credito, data di scadenza, indirizzo di fatturazione ecc.) il numero di poltrona e lo storico delle prenotazioni.

Immigration and Naturalization Service le quali potevano poi condividere i medesimi dati con altre agenzie federali nello scopo di "proteggere la sicurezza nazionale". In altre parole, tali informazioni potevano essere utilizzate da praticamente tutte le agenzie federali USA e ciò risultava in contrasto con il principio di divieto di trasferimento ulteriore[442].

Allo stesso modo il Gruppo di lavoro sottolineava che i dati avrebbero dovuto, comunque, essere trasferiti attraverso un sistema di tipo *push*, laddove il sistema allora in vigore era, invece, di tipo *pull*[443]. Infatti, con il sistema allora in vigore la CBP otteneva i dati PNR attraverso l'accesso diretto ai CRS ancor prima della partenza del volo. Il sistema di tipo *push*, invece, era maggiormente rispettoso della privacy dei passeggeri in quanto erano le compagnie aeree ad inviare i dati direttamente alla CBP e ciò consentiva un filtraggio dei dati sensibili da parte delle compagnie prima di essere inviati alla CBP.

Pertanto, nelle sue conclusioni, il Gruppo di Lavoro invitava la Commissione Europea ad avviare delle discussioni con il Governo degli USA al fine di delimitare con maggiore precisione gli obiettivi della raccolta dei dati, di determinare le tipologie di dati trasferibili e di ottenere garanzie in merito al trattamento ed alla comunicazione dei dati da parte delle agenzie federali. Invero, il riconoscimento in capo alle autorità doganali degli USA del diritto di accedere ai dati raccolti dalle compagnie europee implicava comunque l'attribuzione dell'esercizio di un potere sovrano sul territorio dell'Unione. Un trattato internazionale diveniva allora necessario per esprimere il consenso dell'Unione all'esercizio di una potestà sovrana straniera sul proprio territorio[444].

4. La definizione di un accordo ad interim e la successiva conclusione del primo accordo sui PNR

I negoziati tra la Commissione europea e la CBP furono più complessi di quanto inizialmente previsto ma, in ogni caso, sfociarono nell'adozione di un accordo provvisorio nel gennaio del 2003[445].

Secondo i termini essenziali dell'accordo provvisorio, agli Stati Uniti sarebbe stato concesso di accedere ai dati PNR dei vettori aerei europei. Gli Stati membri, dal canto loro, non avrebbero applicato la direttiva 95/46/CE e le relative disposizioni nazionali di attuazione nei confronti delle

[442] Cfr. Opinion 2/2004 sub nota 34
[443] Idem
[444] Adam "*L'échange de données ò caractère personnel entre l'Union européenne et les Etats Unis. Entre souci de protection et volonté de coopération* » in Revue trimestrielle de droit européen, 2006 p.423
[445] Idem

compagnie aeree che avrebbero ottemperato alle richieste americane e ciò fintantoché le parti non avrebbero trovato un punto di incontro per un accordo bilaterale[446].

Come si noterà, già fin dalla conclusione dell'accordo temporaneo il Governo USA otteneva l'accesso richiesto ai dati PNR senza dover fare alcuna concessione in cambio, mentre la Commissione si trovava, al contrario, nella situazione di dover invitare gli Stati membri a disapplicare la normativa di derivazione comunitaria[447].

Per questo motivo, poco dopo la conclusione dell'accordo *ad interim* il Presidente del Gruppo ex art. 29 inviava una pubblica lettera al Presidente del Comitato su i Diritti e le Libertà dei Cittadini, Giustizia ed Affari Interni del Parlamento Europeo[448] nel quale criticava l'accordo per essere stato concluso senza tenere in considerazione il parere 6/2002[449] reso dal Gruppo di Lavoro e senza consultare quest'ultimo.

Il Gruppo di Lavoro esprimeva, altresì, grande preoccupazione dinnanzi alla prospettiva che una questione di simile delicatezza potesse essere affrontata senza tenere conto dei numerosi rilievi formulati nel citato parere. Per questo motivo Stefano Rodotà chiedeva di posticipare di qualche mese l'applicazione dell'accordo al fine di permettere al Gruppo di lavoro di poter meglio esaminare la questione e fornire così alle parti gli elementi indispensabili ai fini della finalizzazione di un accordo bilaterale in linea con i canoni stabiliti dalla Direttiva 95/46/CE[450].

Nel Marzo 2003 il Parlamento Europeo emanava una risoluzione[451] con la quale manifestava la propria contrarietà all'accordo *ad interim.* In particolare il Parlamento nutriva dubbi sul fatto che i dati comunicati alle autorità di frontiera USA fossero adeguatamente protetti una volta trasferiti nel database americano, posta l'assenza di una decisione della Commissione che constatasse l'adeguatezza del livello di protezione offerto dalla legislazione americana[452].

Allo stesso modo il Parlamento lamentava il ritardo della Commissione nel formulare delle proposte relative ad una serie di problemi che riguardavano la protezione dei dati e che avevano un enorme impatto su altre politiche comunitarie (trasporti ed immigrazione) e dell'Unione (cooperazione di polizia e giudiziaria in materia penale e lotta al terrorismo e al crimine organizzato), nonché di verificare se vi fossero delle effettive ragioni nella legge americana che giustificassero l'accesso ai dati dei passeggeri o se si trattasse di un'interpretazione ampia da parte

[446] Ibidem
[447] Adam, nota. 444
[448] Lettera del Presidente Stefano Rodotà consultabile su http://www.statewatch.org/news/2003/mar/art29ch.pdf
[449] Opinion 6/2002 on transmission of Passenger Manifest Information and other data from Airlines to the United States, consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp66_en.pdf
[450] *EU scheint machtlos in Flugdaten-Affäre*. Heise Online, March 27, 2003. consultabile su http://www.heise.de/newsticker/data/jk-27.03.03-002/
[451] European Parliament resolution on transfer of personal data by airlines in the case of transatlantic flightshttp://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/ce061/ce06120040310en03810384.pdf
[452] Idem

dell'amministrazione dell'epoca[453]. Inoltre, la Commissione non avrebbe fornito informazioni al pubblico il quale avrebbe dovuto essere il primo a sapere che cosa veniva fatto delle informazioni che lo riguardavano.

Ma il Parlamento deplorava con vieppiù vigore il *joint statement* del 19 febbraio 2003 della Commissione e degli Stati Uniti il quale, oltre a difettare di qualsiasi base giuridica, poteva essere interpretato come un invito diretto alle autorità nazionali di controllo sulla protezione dei dati ad ignorare la normativa europea e pertanto invitava la Commissione a sospendere gli effetti delle misure adottate dagli Usa fino all'adozione di una decisione circa la compatibilità delle medesime con il diritto comunitario[454].

Nel dicembre 2003 la Commissione Europea informava il Parlamento circa lo stato dei negoziati con la US Customs and Border Protection. La comunicazione evidenziava l'obiettivo di "*ottenere i migliori standard di protezione possibili per i dati trasferiti dall'Unione Europea e di incorporarli in un apposito quadro legale*"[455]. E' pur vero che, durante i mesi del negoziato, il CBP sarebbe venuto incontro ad alcune richieste della Commissione europea. Ad esempio, i dati sensibili che potevano permettere l'identificazione di un passeggero sulla base della sua religione venivano esclusi dalla lista dei PNR oggetto di trasferimento. Inoltre i passeggeri avrebbero avuto diritto alla rettifica dei propri dati. Tuttavia, le concessioni americane rimanevano insufficienti sotto molti aspetti. Ad esempio il numero dei dati raccolti era sceso da 38 a 34, una quantità di dati comunque da considerarsi eccessiva.

Successivamente, il 1° marzo 2004 la Commissione sottoponeva al Parlamento il progetto di decisione sull'adeguatezza, in virtù dell'art. 25, n. 6, della direttiva[456], accompagnato dal progetto di impegno del CBP. A stretto giro, il 17 marzo 2004 la Commissione trasmetteva al Parlamento, nell'ottica della consultazione di tale organo ai sensi dell'art. 300, n. 3, primo comma, CE, anche una proposta di decisione del Consiglio avente ad oggetto la conclusione di un accordo con gli Stati Uniti in materia di trasferimento dei dati PNR[457]. Secondo le norme all'epoca in vigore il parere del Parlamento non avrebbe, comunque, avuto valore vincolante.

---

[453] Ibidem

[454] Idem, ut supra

[455] http://ec.europa.eu/comm/external_relations/us/intro/apis_en.pdf

[456] European Commission Decision of 14 May 2004 on the Adequate Protection of Personal Data Contained in the Passenger Name Record of Air Passengers Transferred to the United States' Bureau of Customs and Border Protection, 2004 in GUUE L 235 p. 15 reperibile su http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX :32004D0535:EN:HTML

[457] Council Decision 2004/496, On the Conclusion of an Agreement Between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004 O.J. (L 183) 83, disponibile su http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/1_183/1_18320040520en00830083.pdf;

Nel formulare la sua Risoluzione[458] in risposta il Parlamento osservava che la proposta non poteva costituire adeguata base giuridica per effettuare l'operazione di trasferimento dei dati. Allo stesso modo il Parlamento chiedeva alla Commissione di sostituire il sistema pull con un sistema push[459].

Il 28 maggio 2004 Stati Uniti e Unione Europea firmavano un accordo definitivo che consentiva il trasferimento dei dati PNR agli USA[460].

Come si anticipava poc'anzi, l'accordo veniva preceduto da una decisione della Commissione emessa ai sensi dell'art. 25 par. 6 della Direttiva 96/46 con la quale constatava l'adeguatezza del livello di protezione dei dati offerto dal *Department of Homeland Security* sulla base degli *undertakings* inviati alla Commissione[461]. In particolare, nella conferenza stampa successiva all'approvazione della decisione di adeguatezza il Commisssario Bolkestein ammetteva che le autorità americane avevano applicato "*una forte pressione politica*" sulla Commissione al fine di ricevere la decisione di adeguatezza, ma che tuttavia a giudizio del Commissario il risultato negoziato "*era equilibrato*" [462].

In dottrina è stato osservato come la successione di tali atti sia stata quantomeno anomala se raffrontata alla recente prassi applicativa dell'art. 25 par. 6[463]. Fino all'Accordo in discorso, infatti, all'adozione di una decisione sull'adeguatezza non aveva mai fatto seguito un accordo internazionale. In quest'ottica è importante sottolineare che, in questo caso, l'accordo è stato soggetto semplicemente all'approvazione degli Stati membri e partecipanti, altresì, all'organo tecnico, ossia il comitato ex art. 31, che assiste la Commissione durante la procedura di emanazione della decisione sull'adeguatezza. Il Parlamento è stata, pertanto, l'unica istituzione totalmente esclusa da tale processo decisionale ciò nonostante la rilevanza di una decisione di adeguatezza e nonostante il fatto la stessa direttiva fosse stata provata anche dal Parlamento europeo per mezzo della procedura di co-decisione[464].

L'accordo forniva un quadro nell'ambito del quale l'Unione europea era in grado di approvare diverse misure richiesta al fine di rendere il trasferimento dei dati PNR alla US Customs and Border

[458] European Parliament Resolution http://www.europarl.europa.eu/omk/omnsapir.so/calendar?APP=PDF&;TYPE=PV2&;FILE=p0040331EN.pdf&;LANGUE=EN

[459] http://epic.org/privacy/intl/EP_Res-040704.pdf

[460] Press Release, European Commission External Relations, International Agreement on Passenger Name Records (PNR) Enters Into Force (May 28, 2004), available at http://ec.europa.eu/comm/external_relations/us/news/ip04_694.htm.

[461] Cfr. Nota 54 supra

[462] Redazione *Europe bows to US on air passenger data*. International Herald Tribune, 18 maggio 2004

[463] Alfredo Terrasi "*Trasmissione dei dati personali e tutela della Riservatezza:l'accordo tra Unione Europea e Stati Uniti del 2007*" in Rivista di Diritto Internazionale 2008, 2, p. 381

[464] Idem

Protection, compatibile con il diritto europeo[465]. I Dati PNR sarebbero stati raccolti da "*tutte le persone il cui viaggio includeva un volo per o dagli Stati Uniti*" incluse tutte "le *persone transitanti attraverso gli Stati Uniti"*[466]

Inizialmente i dati sarebbero stati soggetti ad un sistema di trasferimento di tipo *pull* entre 72 ore dal decollo del volo. Invero, sebbene il Parlamento europeo e il Gruppo ex art. 29 avessero sostenuto l'opportunità dell'utilizzo del sistema *push*, la Commissione accoglieva la richiesta del DHS di fare ricorso al sistema pull.

I dati raccolti sarebbero stati filtrati al fine di evitare l'uso di taluni dati quali "*i dati personali suscettibili di rivelare l'origine etnica razziale le opinioni politiche religiose o filosofiche, l'appartenenza a sindacati e dati concernenti la salute e la vita sessuale dell'individuo*". Dopo la raccolta i dati sarebbero stati immagazzinati presso la *National Archives and Records Administration* con accesso limitato per tre anni e mezzo, dopo di che sarebbero stati distrutti a meno che non vi fosse stato un accesso da parte della *US Customs and Border Protection*. Ove la CBP avesse fatto accesso a tali dati, questi sarebbero stati trasferiti alla CBP per essere immagazzinati per un periodo addizionale di otto anni[467].

L'accordo finale includeva un a lista di 34 elementi di dati PNR che includevano ampie categorie come "*general remarks*" e "*all historical changes to the PNR*" [468].

Le finalità per l'utilizzo dei dati PNR venivano strettamente limitate a "finalità di prevenzione e lotta: 1) al terrorismo e crimini connessi; 2) altri gravi delitti incluso il crimine organizzato di natura transnazionale 3) evasione o latitanza in relazione ai delitti sopra indicati. Tuttavia l'accordo permetteva al CBP di "*esercitare la sua discrezione al fine di trasferire dati PNR per le finalità indicate*" ad altre agenzie governative incluse le autorità governative di altri paesi. L'accordo specificava che "*nessuna disposizione pregiudicherà il trasferimento di dati PNR ad autorità governative competenti ove tale trasferimento dia necessario per la protezione degli interessi vitali del titolare dei dati o di un'altra persona e "nessuna disposizione in questi Undertakings impedirà l'uso o la condivisione di dati PNR in qualsiasi procedimento penale o diversamente quando richiesto dalla legge"*.

L'accordo veniva adottato sulla base dell'art. 95 in quanto nell'ottica del Consiglio, in assenza di una normativa comune in tema di accesso da parte delle autorità statunitensi ai dati PNR

[465] Agreement between the European Community and the United States of America on the Processing and Transfer of PNR Data by Air Carriers to the United States Department of Homeland Security, Bureau of Customs and Border Protection, 2004 O.J. (L 183) 84, available at http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/1_183/1_18320040520en00840085.pdf.
[466] Idem
[467] Ibidem
[468] Pascal KAMINA Accord sur les données des passagers des compagnies aériennes Communication Commerce électronique n° 9, Septembre 2004, Alerte 181

sussisteva il rischio che venissero falsate le condizioni di concorrenza con grave pregiudizio all'unicità del mercato interno. Secondo detta visione, infatti, le compagnie aeree che non si sarebbero confermate alle esigenze degli USA avrebbero potuto vedersi imporre, da parte delle autorità americane, il pagamento di ammende, e perdere passeggeri a vantaggio di altre compagnie che si fossero accordate con gli Stati Uniti.

5. L'opposizione del Parlamento europeo

I negoziati volti alla conclusione del primo accordo internazionale sui PNR scatenavano le critiche profonde del Parlamento Europeo e di vasti segmenti della società civile[469].

Già il 14 aprile 2004, infatti, il Parlamento, che sarebbe rimasto poi escluso dalla conclusione dell'accordo internazionale in quanto adottato sulla base dell'art. 300 del TCE[470], emanava una risoluzione che riguardava, oltre che l'accordo PNR, anche l'affare Swift, mediante la quale criticava la mancanza di trasparenza nella gestione, da parte della Commissione Europea, del dialogo transatlantico su questioni che riguardavano il diritto fondamentale alla protezione dei dati[471].

Allo stesso modo, sempre nell'aprile del 2004, il Parlamento Europeo avanzava una richiesta di parere alla Corte di Giustizia[472] in merito a due questioni relative all'accordo: 1) se l'acquisizione di dati da parte della Customs and Border Protection costituisse esercizio di un potere sovrano da parte degli Stati Uniti nei confronti delle nazioni europee e 2) se l'accordo violasse la direttiva 95/46 permettendo il trattamento di dati personale ai sensi di obblighi giuridici imposti da una nazione terza[473].

Tuttavia, nel luglio 2004, dato che la Commissione aveva proceduto alla conclusione dell'accordo senza l'approvazione (peraltro non vincolante) del Parlamento Europeo e senza

[469] *EU-US PNR: Council to ignore Parliament and go ahead with "deal*" reperibile su http://www.statewatch.org/news/2004/may/06eu-us-nr-deal.htm

[470] In base a tale articolo i trattati internazionali approvati in settori in cui a livello interno si applicava la procedura di co-decisione prevista dall'art. 251 TCE venivano ratificati dal Consiglio su proposta della Commissione. Il parlamento svolgeva una funzione consultiva ma il suo parere non era vincolante. Tuttavia il secondo comma dell'art. 300 prevedeva che nel caso in cui l'accordo comportasse la modifica di una norma Comunitaria precedentemente approvata con la procedura di co-decisione, il Parlamento doveva fornire il suo assenso con valore vincolante alla ratifica dell'accordo da parte del Consiglio.

[471] Marc-Antoine LEDIEU « *L'adoption de la résolution sur les données des passagers et l'affaire SWIFT »* Communication Commerce électronique n° 4, Avril 2007, alerte 79

[472] Parere n° 1/04 : GUUE C 118, 30 aprile 2004, p. 1

[473] Paul Meller, *Europe Asks Court to Rule on Air Security Pact*, N.Y. TIMES, Apr. 22, 2004.

attendere che la Corte di Giustizia si esprimesse sulla questione, il Parlamento ritirava le richieste di parere e presentava ben due ricorsi alla Corte di Giustizia in data 27 luglio 2004.

In particolare, nella causa iscritta al numero C-317/04 il Parlamento chiedeva l'annullamento della decisione n° 2004/496/CE del Consiglio del 17 maggio 2004 concernente la conclusione dell'accordo[474].

Nella causa iscritta al numero C-318/04, invece, il Parlamento mirava a censurare la decisione n° 2004/535/CE, della Commissione, del 14 maggio 2004 relativa al livello adeguato di protezione dei dati personali contenuti nei dossier passeggeri trasferiti al'Ufficio delle Dogane e della Protezione delle Frontiere USA [475].

Nell'impugnativa proposta il Parlamento Europeo veniva sostenuto dal Garante Europeo per la Protezione dei dati che, per la prima volta nella sua storia, partecipava ad un giudizio innanzi alla Corte di Giustizia[476]. Parallelamente, nella causa C-318/04, con ordinanza del presidente della Corte 17 dicembre 2004, veniva ammesso l'intervento del Regno Unito a sostegno delle conclusioni della Commissione.

Il Parlamento chiedeva che i ricorsi venissero trattati con la procedura d'urgenza ai sensi dell'art. 62 del Regolamento di procedura della Corte. Tuttavia, il Presidente della Corte, con ordinanza del 21 settembre 2004 pubblicata solamente in ottobre, respingeva tale richiesta, atteso che la stessa risultava insufficientemente motivata sotto il profilo dell'urgenza e che, il Parlamento non aveva chiesto delle misure di sospensione delle decisioni impugnate[477]. In ogni caso come osservato in dottrina, il rigetto della richiesta di procedura urgente avanzata dal Parlamento non deponeva già affatto bene con riferimento alle prospettive di accoglimento dei ricorsi, sia con riferimento all'utilità di un giudicato che, a causa dei tempi richiesti dalla procedura ordinaria, sarebbe arrivato comunque dopo almeno tre anni e con riferimento ad un accordo internazionale valevole, esso pure, per tre anni![478]

In considerazione della connessione tra tali cause, confermata nella fase orale, i procedimenti in esame venivano riuniti ai fini della decisione a norma dell'art. 43 del regolamento di procedura della Corte.

6. La sentenza di annullamento della Corte di Giustizia

[474] Cfr. GUUE n° L 183, 20 maggio 2004, p. 83-85
[475] Cfr. GUUE n° L 235, 6 luglio 2004, p. 11-22
[476] Cfr. Paskal KAMINA, nota 468
[477] Flavien MARIATTE « *Rejet par la Cour des demandes de traitement accéléré des recours dans le dossier du transfert des données* PNR » in Revue Europe n° 12, Décembre 2004, comm. 400
[478] Marc-Antoine LEDIEU « *Accord PNR - Pas d'urgence pour la CJCE »* Communication Commerce électronique n° 1, Janvier 2005, Alerte 22

6.1 La decisione sulla causa C-318/04 Parlamento c. Commissione

Nel maggio del 2006, a ben due anni di distanza dal deposito dei ricorsi per annullamento promossi dal Parlamento Europeo, la Corte di Giustizia emetteva la propria decisione in merito allo *status* dell'Accordo tra Stati Uniti ed Unione Europea sul trasferimento dei dati PNR[479].

In particolare, con riferimento alla prima causa (C-318/04) vertente sulla richiesta di annullamento della decisione di adeguatezza della Commissione, la Corte osservava che l'art. 3 par. 2 della Direttiva 95/46/CE "*esclude dal suo ambito di applicazione i trattamenti di dati personali effettuati per l'esercizio di attività che non rientrano nell'ambito del diritto comunitario*" quali " *i trattamenti riguardanti la sicurezza pubblica, la difesa, la Sicurezza dello Stato e le attività statali nel campo del diritto penale*". (v. punto 54 della decisione).

Ciò premesso, la Corte rilevava come la decisione sull'adeguatezza della Commissione riguardasse solamente la trasmissione dei dati PNR alla Customs and Border Protection sulla base della legge americana e dei relativi regolamenti di attuazione. Inoltre, la Corte osservava, altresì, come quest'ultima legislazione avesse ad oggetto "*il rafforzamento della sicurezza, nonché le condizioni di ingresso negli Stati Uniti e di uscita dal paese*", e che i considerando della decisione prevedevano il sostegno della Comunità agli Stati Uniti "*nella loro lotta contro il terrorismo nei limiti imposti dal diritto comunitario*", oltre che l'utilizzo dei dati PNR allo scopo di prevenire e combattere il terrorismo e gli altri gravi reati transnazionali, ivi compresa la criminalità organizzata[480].

Sulla scorta di tale premessa la Corte rilevava, dunque, come il trasferimento dei dati PNR alla *Customs and Border Protection* statunitense, così come previsto dall'accordo in esame, non rispondesse allo scopo di fornire dei servizi di tipo commerciale, bensì configurasse "*un trattamento avente come oggetto la pubblica sicurezza e le attività dello Stato in materia di diritto penale*[481]".

In larga parte, dunque, la succinta motivazione della decisione della Corte di Giustizia seguiva la raccomandazione contenuta nelle conclusioni rassegnate dall'Avvocato Generale Philippe Léger, secondo cui « *le fait que les données PNR ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un États tiers* », non implicava affatto che questo trasferimento potesse essere riconducibile al campo di applicazione

[479] Cfr. Corte di Giustizia, in cause riunite C-317/04 e C-318/04, Parlamento c. Consiglio e Commissione, Sentenza del 30 maggio 2006 disponibile su http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62004J0 317:EN:HTM
[480] cfr. punto 55 della decisione
[481] cfr. punto 56 della decisione

della Direttiva. Quest'ultimo, infatti, finiva con l'inserirsi *« dans un cadre institué par les pouvoirs publics et visant la sécurité publique*[482] *»*

Non era la prima volta che la Corte di Giustizia si pronunciava sul campo di applicazione *ratione materiae* della Direttiva. Come si è visto precedentemente, infatti, già nella sentenza Lindqvist, richiamata dalla decisione in esame, la Corte aveva preso posizione sulla portata dell'art. 3 par. 2 della Direttiva, chiarendo per un verso il carattere meramente esemplificativo dell'elencazione ivi contenuta e, per l'altro, che i trattamenti di dati esclusi dal campo di applicazione della Direttiva fossero quelli correlati allo svolgimento di "*attività proprie degli Stati o delle autorità statali estranee ai settori di attività dei singoli*"[483].

In altre parole, nel caso in esame la sentenza della Corte, sulla scorta di quanto deciso in *Lindqvist*, implicava sostanzialmente che è la finalità del trasferimento effettuato, e non già la natura o l'origine dei dati, a determinare l'oggetto e la natura del loro trattamento[484]. Invero, come sottolineava l'avvocato generale, le cui conclusioni sono un pò più precise rispetto a quelle della Corte, « la *Commission ne disposait pas, en vertu de l'article 25 de la directive n° 95/46, du pouvoir d'adopter une décision relative au niveau de protection adéquat de données à caractère personnel transférées dans le cadre et en vue d'un traitement exclu expressément du champ d'application de ladite directive* ».

Sulla scorta delle suesposte osservazioni, pertanto, la Corte concludeva che la Direttiva 95/46/CE non poteva fondare la competenza della Comunità per la conclusione dell'Accordo e che la decisione di adeguatezza "*doveva pertanto essere annullata*".

La Corte non si pronunciò, invece, sui restanti motivi di ricorso del Parlamento riguardante i profili di violazione della Convenzione Europea dei Diritti Fondamentali o sulle altre disposizioni a tutela della privacy contenute nella Direttiva.

6.2 La decisione sulla causa C-317/04 Parlamento c. Consiglio

Quanto alla seconda causa (C-317/04) successivamente riunita, Il Parlamento sollevava cinque motivi a sostegno del suo ricorso avverso la decisione n. 2004/496/CE del Consiglio[485].

[482] Conclusioni dell'Avvocato Generale Philippe Léger in cause riunite C-317/04 e C-318/04 del 22.11.2005 punto 73.
[483] Cfr. C-101/01 Lindqvist, sentenza del 6 novembre 2003, punto 43
[484] Filippo Fontanelli, *La Corte di Giustizia e il "Favor Communitatis".Il percorso della giurisprudenza della Corte di Giustizia delle Comunità Europee sul fondamento normativo degli atti della Comunità e dell'Unione"* in Rivista Italiana di Diritto Pubblico Comunitario, 2010, 1 p. 183 e ss
[485] Communication au journal officiel Recours introduit le 27 juillet 2004 contre le Conseil de l'Union européenne

Nei primi due motivi il Parlamento contestava il fondamento normativo della decisione impugnata. In primo luogo, il Parlamento riteneva che l'utilizzo dell'art. 95 CE non fosse giustificato, alla luce, in particolare, della recente giurisprudenza della Corte su tale disposizione; del resto, l'art. 95 CE non era idoneo a fondare la competenza della Comunità a concludere l'accordo, in quanto quest'ultimo riguardava il trattamento di dati esclusi dall'ambito di applicazione della direttiva 95/46/CE sulla tutela dei dati personali. Inoltre, oggetto dell'accordo medesimo non sarebbe stata né l'instaurazione, né il funzionamento del mercato interno, né tantomeno la rimozione di ostacoli alla libera prestazione dei servizi. Inoltre, la decisione censurata non conteneva neppure delle disposizioni tendenti alla realizzazione di un tale obiettivo. In altre parole, sempre secondo il Parlamento, unico scopo della decisone sarebbe stato quello di legittimare il trattamento di dati personali quale imposto dalla legislazione statunitense[486].

Nel secondo e terzo motivo il Parlamento sottolineava come l'accordo implicasse una modifica di una direttiva, adottata secondo la procedura di co-decisione di cui all'art. 251 CE e che, pertanto, esso poteva essere concluso solo previo parere conforme del Parlamento. Allo stesso modo, il Parlamento sosteneva che l'accordo era stato concluso in violazione dei diritti fondamentali, in particolare del diritto alla tutela dei dati personali, e che esso costituiva altresì un'ingerenza ingiustificata nella vita privata, come tale incompatibile con l'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[487]. Sotto questo profilo il Parlamento adduceva l'assenza di una motivazione sufficiente per un atto che presentava caratteristiche così particolari[488].

Il quarto ed ultimo motivo, invece, riguardava la violazione del principio di proporzionalità, in particolare per il fatto che l'accordo prevedesse il trasferimento di una quantità eccessiva di dati dei passeggeri e che tali dati venissero conservati troppo a lungo dalle autorità americane, nonché la violazione del principio di leale collaborazione previsto all'art. 10 CE, alla luce delle circostanze alquanto insolite in cui era avvenuta l'adozione della decisione impugnata, che è intervenuta nel corso della procedura di domanda di parere 1/04 dinanzi alla Corte di giustizia[489].

Il Consiglio, nel suo controricorso, sosteneva che l'accordo avrebbe riguardato la libera circolazione dei dati PNR tra la Comunità e gli Stati Uniti in condizioni che rispettavano le libertà e i diritti fondamentali delle persone, in particolare la vita privata. Inoltre, l'accordo sarebbe stato

---

par le Parlement européen (affaire C-317/04)
http://curia.europa.eu/juris/document/document.jsf?docid=52220&mode=req&pageIndex=1&dir=&occ=first&part=1&text=&doclang=FR&cid=2017221

[486] cfr. punto 63 della decisione

[487] idem

[488] « *L'accord UE/USA sur le transfert des données passagers aux bons soins de la Cour »,* Révue Europe n° 10, Octobre 2004, Alerte 34

[489] Cfr. nota 84 supra

diretto a sopprimere qualsiasi distorsione della concorrenza tra le compagnie aeree degli Stati membri e fra queste ultime e le compagnie degli Stati terzi, che poteva derivare dalle condizioni imposte dagli Stati Uniti. Invero, nel'ottica del Consiglio, le condizioni della concorrenza "*avrebbero potuto essere falsate per il fatto che solo alcune di asse avrebbero accordato alle autorità statunitensi un accesso alle loro banche dati. L'accordo intenderebbe imporre obblighi uniformi a tutte le compagnie interessate*"[490].

La Commissione, invece, sottolineava l'esistenza di un «conflitto di leggi», nel senso del diritto internazionale pubblico, tra le leggi degli Stati Uniti e la normativa comunitaria oltre che la necessità di conciliarle e rilevava come l'art. 95 costituisse «fondamento normativo naturale» della decisione, in quanto l'accordo avrebbe riguardato la dimensione esterna della protezione dei dati personali nel momento del loro trasferimento all'interno della Comunità. Gli artt. 25 e 26 della direttiva avrebbero, dunque, fondato una competenza esclusiva esterna a favore della Comunità. Inoltre, la Commissione sosteneva che il trattamento iniziale di quei dati da parte delle compagnie aeree avesse finalità commerciali. L'uso che ne avrebbero fatto in seguito le autorità statunitensi non li avrebbe sottratti all'incidenza della Direttiva[491].

La Corte di Giustizia, investita di tutte le suesposte questioni, si limitava a constatare con motivazione perplessa, che l'art. 95 CE letto in combinazione con l'art. 25 della Direttiva non era suscettibile di fondare la competenza della Comunità per concludere l'accordo in quanto esso *"ha come obiettivo il medesimo trasferimento di dati che la decisione di adeguatezza e quindi dei trattamenti dei dati che sono ... esclusi dal campo di applicazione della direttiva*"[492]. Conseguentemente, la decisione 2004/496/CE non era stata validamente adottata sul fondamento dell'art. 95 TCE e doveva, pertanto, essere annullata.

A questo punto la Corte giudicava inutile esaminare gli ulteriori motivi di ricorso avanzati dal Parlamento. L'accordo sarebbe rimasto, tuttavia, applicabile anche a seguito della decisione per un termine di novanta giorni per ragioni di certezza del diritto e al fine di proteggere le persone interessate e dunque fino al 30 settembre 2006[493].

7. Osservazioni critiche in merito alla decisione della Corte di Giustizia

[490] cfr. punto 64 decisione
[491] Cfr. punto 65 della decisione
[492] Pt 67-69.
[493] *Annulation d'un accord CE/USA sur le traitement et le transfert de données à caractère personnel par des transporteurs aériens* La Semaine Juridique Entreprise et Affaires n° 23, 8 Juin 2006, act. 264

Numerose osservazioni e critiche sono state formulate in dottrina con riguardo alla sentenza della Corte di Giustizia in merito all'accordo PNR.

Effettivamente ciò pare giustificarsi col fatto che il caso PNR presenta, comunque, un rilevante interesse sotto un profilo giuridico, proprio perché ben esemplifica le specificità proprie del patrimonio europeo in tema di protezione dei dati personali rispetto ad altre tradizioni giuridiche ed in particolare, rispetto alla tradizione americana.

Al contempo, è stato efficacemente osservato come esso evidenzi le aporie e le asimmetricità che, in tema di protezione dei dati personali, discendevano dal previgente assetto istituzionale dell'Unione Europea suddiviso in distinti pilastri che ne definivano, spesso limitandola, la latitudine del potere di intervento[494].

Ciò premesso, l'analisi contenuta nella sentenza della Corte, per la sua sinteticità, è stata giudicata dalla dottrina come la più rapida e la più condensata di tutta la storia del contenzioso vertente sulla scelta della base giuridica, quantomeno degli accordi internazionali[495].

Inoltre, è stato osservato come il contenzioso innanzi alla Corte di Giustizia sul tema dell'accordo PNR non costituisca una novità giurisprudenziale, ma come esso si collochi nel quadro del più ampio fenomeno dei conflitti tra le istituzioni politiche europee[496], il quale può manifestarsi anche e soprattutto attraverso il contenzioso sul fondamento giuridico degli atti comunitari[497].

In ogni caso, è stato evidenziato dalla dottrina come la decisione in esame, che ha ritenuto di censurare la scelta di un fondamento normativo nell'ambito del primo pilastro ai fini dell'annullamento di un atto adottato *ultra vires*, rappresenti un caso unico nell'ambito di una giurisprudenza che, di regola, ha sempre teso ad affermare la legittimità o, comunque, la

---

[494] *"Sicurezza e protezione dei dati personali nell'Unione Europea:le aporie del sistema alla luce dei casi PNR e Irlanda (caso data retention)"* in Cassazione Penale 2010, 1 p. 1281

[495] Corte di Giustizia, 27 sept. 1988, causa C-165/87, Commissione c/ Consiglio : Racc. 1988, p. 5545, Convenzione internazionale sul sistema armonizzato di designazione e di codificazione delle merci. – Corte di Giustizia, 7 marzo 1995, causa C-360/93, Parlamento c/ Consiglio : Racc.1996, I, p. 1195, Accord CEE/USA concernant la passation de marchés publics. – Corte di Giustizia, 3 dicembre 1996, causa C-268/94, Portogallo c/ Consiglio : Racc. 1996, I, p. 6177, Accordo do cooperazione con l'India. – Corte di Giustizia, 8 luglio 1999, causa C-189/97, Parlamento c/ Consiglio: Racc. 1999, I, p. 4741, Accordo CE/Mauritania di cooperazione in materia di pesca marittima. – Corte di Giustizia , 30 gennaio 2001, causa C-36/98, Spagna c/ Consiglio : Racc. CJCE 2001, I, p. 779, Convenzione sulla cooperazione per la protezione e l'utilizzo durevole del Danubio. – Corte di Giustizia , 12 dicembre. 2002, causa C-281/01, Commissione c/ Consiglio : Racc. 2002, I, p. 12049.

[496] Luigi Sbolci, "Conflitti tra Istituzioni dell'Unione Europea e Accordi Interistituzionali" Rivista di Diritto Internazionale, 2007,2, 9. 345

[497] Lucia Serena Rossi "*Costituzionalizzazione" dell'UE e dei diritti fondamentali*", in "*Carta dei Diritti fondamentali e Costituzione dell'Unione Europea"* (a cura di Lucia Serena Rossi) Milano 2002, p. 263 e ss.

preferibilità della base normativa comunitaria rispetto a quelle radicate nel secondo o terzo pilastro[498].

Sono esempio di questa tendenza le sentenze emesse dalla Corte nei casi relativi alle sanzioni penali in tema di illeciti ambientali nel 2005 e 2007[499] in occasione delle quali la Corte come è noto, ha annullato due decisioni quadro del Consiglio[500] recanti istruzioni agli stati membri circa l'obbligo di reprimere penalmente alcune condotte pregiudizievoli per l'ambiente, tra cui l'inquinamento provocato dalle navi.

Invero, in linea generale la giurisprudenza della Corte sembra aver sempre preferito tutelare le attribuzioni della Comunità nei confronti dell'esercizio di ogni genere di poteri da parte degli Stati membri al di fuori del contesto del Trattato CE, di talché l'adozione di un atto sulla base del trattato UE, anche nel panorama pre-Lisbona, doveva considerarsi preclusa anche nei settori di competenza comunitaria concorrente o complementare. Ciò equivaleva, in altre parole, a privilegiare l'azione della comunità rispetto agli altri strumenti di cooperazione intergovernativa in seno all'Unione Europea[501]. Successivamente, questo test messo a punto dalla Corte per valutare la correttezza del fondamento normativo di un atto legislativo è stato raffinato nella successiva giurisprudenza ECOWAS e Kadi[502]

Ferme restando le suesposte considerazioni, occorre sottolineare, altresì, che la decisione della Corte di Giustizia ha suscitato una valanga di critiche da parte di numerosi commentatori, le quali muovono essenzialmente dalla constatazione del fatto che la Corte avrebbe adottato una soluzione dal contenuto sostanzialmente pilatesco, enigmatico quanto ai presupposti e problematico quanto alle conseguenze[503].

Innanzitutto, la decisione è stata criticata da più fronti in ragione del fatto che essa, nell'esaminare esclusivamente il motivo riguardante la correttezza della base giuridica, ha del tutto omesso di prendere posizione in merito agli altri motivi di carattere sostanziale riguardanti la tutela dei diritti fondamentali sollevati dal Parlamento Europeo, evitando così di ricostruire un principio generale di diritto comunitario relativo alla tutela dei dati[504].

---

[498] Filippo Fontanelli, nota 484

[499] CGE 13 settembre 2005, Causa C-176/03 Commissione c- Consiglio dell'Unione Europea in Racc. p. I 7879 e 23 ottobre 2007, causa C-440/05 Commissione c.Consiglio dell'Unione Europea, in Racc. p.I 9097

[500] Decisione Quadro 2003/80/GAI del Consiglio del 27 gennaio 2003 relativa alla protezione dell'ambiente nel diritto penale (in GUUE 2003 L 29 p. 55) e decisione quadro 2005/667/GAI del Consiglio del 12luglio 2005 intesa a rafforzare la cornice penale per la repressione dell'inquinamento provocato dalle navi (in GUUE 2005 L 255 p. 164)

[501] M. Gisella Garbagnati Ketvel, *La giurisprudenza della Corte comunitaria in materia penale: verso un ravvicinamento tra i pilastri dell'Unione Europea*, in Diritto dell'Unione Europea, 2007, 2 p. 399

[502] Idem.

[503] Flavien MARIATTE *La sécurité intérieure des États-Unis... ne relève pas des compétences externes des Communautés* in Révue Europe n° 7, Juillet 2006, étude 8

[504] Alfredo Terrasi , nota 463

Trattasi dell'omissione senz'altro più vistosa della sentenza in questione, in quanto rappresenta un'occasione perduta per definire la portata ed il contenuto della dimensione esterna della tutela dei dati personali nel diritto comunitario. In quest'ottica, la sentenza è motivo di frustrazione non tanto per quello che dice, quanto per ciò che avrebbe potuto dire e che ha omesso di dire[505].

Allo stesso modo, la Corte ha omesso di pronunciarsi in merito al motivo di ricorso sollevato dal Parlamento Europeo con riguardo alla violazione del principio di leale cooperazione istituzionale, sul presupposto che il Consiglio avrebbe scelto di adottare la decisione senza attendere l'esito della richiesta di parere avanzata dal Parlamento[506].

In secondo luogo, la decisione della Corte è stata criticata in quanto, pur annullando la decisione di conclusione dell'accordo, sul presupposto che la stessa era stata adottata in virtù di una non corretta base giuridica, essa non contiene alcuna indicazione circa la base giuridica ritenuta più appropriata[507]. Sotto questo profilo, infatti, la mera constatazione del fatto che un'attività non ricade nell'ambito di applicazione della Direttiva 95/46/CE non implica necessariamente che tale attività debba essere per forza regolata nell'ambito del terzo pilastro ben potendo essere possibile, anche nella constatata assenza di altre disposizioni suscettibili di fondare una competenza della Comunità in materia di lotta al terrorismo, ricorrere comunque all'*estrema ratio* di cui all'art. 308 CE, in tema di esercizio delle competenze sussidiarie[508]. Anche sotto questo profilo, dunque, la sentenza della Corte di Giustizia ha omesso del tutto di pronunciarsi

Ma vi è di più.

Escludendo che alla materia del trasferimento dei PNR alle autorità statunitensi si potessero applicare i principi sul trattamento dei dati contenuti della Direttiva 95/46/CE la Corte ha finito col creare uno spazio in cui le istituzioni europee, in sede di negoziazione di un nuovo accordo con gli USA, avrebbero potuto agire sostanzialmente *legibus solutae*, in mancanza di indicazioni circa gli *standard* minimi di tutela da garantire alla luce del diritto comunitario[509].

Sotto questo profilo, proprio alla luce dei motivi ora esposti, la decisione appare ancor più criticabile se si considera che essa ha sostanzialmente spianato la strada alla conclusione di un accordo fondato sul terzo pilastro in cui, come si vedrà meglio in prosieguo, le garanzie per i diritti fondamentali sarebbero state ulteriormente ridotte.

---

[505] Valerie Michel « La *dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration* », note sous l'arrêt su 30 mai 2006, Parlement européen c. Conseil, aff. jtes C-317 et 318/04, Révue Trimestrielle Droit Européen, 3/2006, p.535

[506] Cfr. Flavien MARIATTE, nota 503

[507] idem

[508] Cfr. *EDPS opinion on the final report by the EU US High Level Contact Group on Information Sharing and Privacy and Personal Data protection*. Paragrafo 22 reperibile su www.edps.europa.eu

[509] Cfr. Alfredo Terrasi , nota 463

Inoltre, con tale decisione la Corte ha permesso la successiva stipula di un nuovo accordo sulla base degli articoli 24 e 38 del TUE i quali,notoriamente, non prevedono l'intervento del Parlamento Europeo, né una possibilità di sindacato da parte della Corte di Giustizia.

Infine, la decisione ha destato particolare attenzione per i possibili esiti cui poteva condurre anche con riferimento ad un altro caso riguardante un distinto provvedimento decisivo della strategia europea nella lotta al terrorismo, ossia la direttiva 2006/24/CE del Consiglio e del Parlamento Europeo "*riguardante la conservazione di dati generali o trattati nell'ambito della fornitura di servizi di comunicazione*" (cd. *data retention directive*) emanata per introdurre alcune disposizioni specificamente orientate ad innalzare, nel quadro della lotta al terrorismo, il livello e le modalità di trattamento e di conservazione dei dati prodotti nell'ambito delle comunicazioni elettroniche[510].

L'Irlanda (sostenuta dalla Slovacchia) aveva, infatti promosso un ricorso per annullamento contro detta direttiva, ritenendo che la stessa non fosse finalizzata migliorare il funzionamento del mercato interno bensì a favorire la raccolta di dati esclusivamente per scopi di sicurezza pubblica e lotta al terrorismo. Forte del precedente relativo al caso PNR, l'Irlanda si sarebbe aspettata un annullamento dell'atto impugnato, sul presupposto dell'errata individuazione della base giuridica nell'art. 95 TCE. Tuttavia, con notevole stupore di tutti i commentatori, la Corte di Giustizia, Grande Sezione ha sancito, che l'art. 95 TCE costituiva una base giuridica del tutto adeguata per la direttiva *data retention*.[511] Tale ultima pronuncia della Corte di Giustizia ha ulteriormente accentuato le perplessità dei commentatori circa la portata della precedente decisione sulla vicenda PNR.

A parere di chi scrive, sebbene la sentenza sia stata generalmente criticata come un segnale di indebolimento dell'Europa sul versante della tutela dei dati, sottratti per effetto della decisione della Corte alla protezione della Direttiva madre, la sentenza stessa ha avuto il merito di aprire uno spaccato su di un palese vuoto normativo, ossia quello riguardante la tutela dei dati personali nel campo della lotta al terrorismo ed alla criminalità organizzata. In quest'ottica, tale sentenza ha confermato quantomeno l'urgenza di comunitarizzare il terzo pilastro al fine di rinforzare il controllo democratico del Parlamento europeo nel settore della lotta al terrorismo e della cooperazione di polizia e giudiziaria in materia penale.

[510] La direttiva cd. "data retention" ha come scopo l'armonizzazione degli obblighi di conservazione dei dati di traffico da parte dei fornitori dei servizi di telecomunicazione per finalità di accertamento e repressione di gravi reati. Di conseguenza essa impone ad operatori e providers di tutta Europa la registrazione per un minimo di sei mesi fino ad un massimo di due anni dei degli accessi internet dei mittenti e dei destinatari delle email e delle telefonate della localizzazione di chi chiama da un celllulare.

[511] Cfr. Flavien MARIATTE, nota 503

In ogni caso, chi scrive sente comunque di condividere l'opinione di chi si sarebbe aspettato un ruolo meno di retroguardia della Corte nel vestire i panni di un vero e proprio giudice costituzionale nella definizione dei confini della protezione dei dati personali anche nell'ambito del terzo pilastro, un ruolo che pure in anni recenti in non pochi casi la Corte ha mostrato di voler interpretare di buon grado[512].

8. Le reazioni degli Stati Uniti e la negoziazione di un nuovo accordo

Come osservato dall'allora Commissario alla Giustizia Franco Frattini la Corte si era pronunciata esclusivamente in merito alla base giuridica dell'Accordo e non sulla sostanza del medesimo[513]. Una simile constatazione non giungeva inaspettata. Effettivamente il silenzio serbato dalla Corte di Giustizia in merito ai profili sostanziali concernenti la tutela dei diritti fondamentali sollevati dal Parlamento nei due ricorsi, consentiva a quel punto alla Commissione ed al Consiglio di agire senza porsi troppo il problema del livello di protezione dei dati offerto dall'accordo e di superare, così numerose delle obiezioni del Parlamento Europeo[514].

Nel giugno del 2006, la Commissione, in risposta alla sentenza della Corte di Giustizia assumeva due importanti iniziative. Da un lato raccomandava al Consiglio di attivarsi al fine di recedere entro la fine del mese dall'accordo vigente, posto che esso avrebbe cessato di applicarsi 90 giorni dopo la denuncia di una delle parti. Al contempo, chiedeva al Consiglio l'autorizzazione ad intavolare i negoziati volti alla stipula di un nuovo accordo con gli Stati Uniti sull'uso dei PNR sulla base dell'art. 38 TUE, posto che il terzo pilastro si presentava come l'unico contesto giuridico corretto per concludere un accordo internazionale vertente su questioni di pubblica sicurezza e di diritto penale.

La Commissione invitava quindi gli USA a risedersi ai tavoli del negoziato durante il corso dei quali un accordo temporaneo sarebbe stato siglato al fine di evitare interruzioni nel traffico aereo nel frattempo che i termini di un nuovo e permanente accordo sarebbero stati finalizzati.

[512] Cfr. Alfredo Terrasi, nota 463
[513] Commento del Commissario alla Giustizia Franco Frattini in merito alla decisione della Corte di Giustizia sulla vicenda PNR http://www.eurunion.org/News/press/2006/20060108.htm
[514] Valerie Michel, nota 505

Sebbene Stati Uniti e Unione Europea non riuscirono a rispettare la scadenza del 30 settembre imposta dalla decisione della Corte di Giustizia, un accordo temporaneo veniva finalizzato nell'ottobre 2006 e destinato a scadere il 31 luglio 2007[515].

L'accordo temporaneo era significativamente più corto e meno dettagliato rispetto a quello precedente. Tuttavia i suoi contenuti erano assai più deteriori per la privacy individuale rispetto alla versione precedente.

In particolare l'accordo temporaneo dilatava notevolmente il numero di agenzie federali abilitate ad ottenere i dati PNR aggiungendo, oltre al CBP e alla US immigration and Customs Enforcement anche l'Office of the DHS Secretary e tutte le entità che direttamente lo sostengono. Esso, inoltre, manteneva il sistema pull per accedere ai dati PNR .[516]

La dottrina ha osservato come il nuovo accordo temporaneo pervenisse al medesimo risultato del precedente in quanto il suo obiettivo era comunque quella di permettere alle autorità americane di accedere per via elettronica ai dati PNR[517].

Successivamente, nel giugno 2007, ovvero un mese prima che l'accordo temporaneo scadesse, la Commissione Europea e il US DHS re-intavolarono le discussioni volte a concludere un accordo definitivo. I negoziati non furono agevoli, in quanto vedevano, dietro le quinte, un Parlamento europeo molto attento e, sul versante americano, delle autorità competenti in materia di sicurezza del territorio sempre più esigenti[518].

In ogni caso, in seguito a tali negoziati, le parti raggiunsero un accordo definitivo per il trasferimento ed il trattamento di dati PNR detenuti dalle compagnie che entravano nello spazio aereo USA al CBP[519].

L'accordo veniva firmato il 23 luglio 2007 a Bruxelles ed il 26 luglio 2007 a Washington con scadenza al luglio 2012.

L'accordo permanente focalizzava alcune delle criticità e delle problematiche riscontrate nei precedenti accordi. Esso si fondava, ai sensi del punto primo, sulle "garanzie" fornite in una lettera indirizzata dal Ministro dell'Interno DHS, all'Unione Europea, contenente le modalità attraverso

[515] Press Release, U.S. Dept. of Homeland Security, Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Agreement with European Union (Oct. 6, 2006), available at http://www.dhs.gov/xnews/releases/pr_1160772588688.shtm; EU Further Loosens Data Protection and Privacy Rules to Fight Terrorism, INTERNET BUS. L. SERVS., Nov. 20, 2006.

[516] *Ad Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record Data*, 72 Fed. Reg. 348 (Jan. 4, 2007).

[517] Flavien MARIATTE Transfert *des données PNR et protection des données personnelles* Europe n° 12, Décembre 2006, comm. 359

[518] Loïc GRARD *Transfert de données personnelles des passagers* Revue de droit des transports n° 9, Octobre 2007, comm. 197

[519] Comunicato stampa, U.S. Dept. of Homeland Security*, Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Data*, (5 luglio 2007), consultabile su http://www.dhs.gov/xnews/releases/pr_1183667401959.shtm.

cui il DHS assicurava la raccolta l'utilizzo e lo stoccaggio dei dati PNR. Queste garanzie erano formalmente prese in considerazione da una lettera di risposta dell'UE agli USA in quanto permettenti di ritenere che il DHS assicurava un adeguato livello di protezione dei dati PNR. Le due lettere venivano allegate all'accordo.

Ai sensi dell'accordo definitivo, le compagnie aeree dell'UE avrebbero dovuto comunicare alle autorità americane 19 tipi di dati PNR, dopo aver realizzato un sistema di esportazione dei dati conforme alle esigenze tecniche del DHS[520]. In mancanza, il DHS si riservava comunque la possibilità di accedere in via diretta ai sistemi di prenotazione delle compagnie sulla base del meccanismo *pull* previsto dal il primo accordo.

In altri termini il nuovo accordo privilegiava un sistema *push* anziché *pull*, sebbene l'accordo precisasse che la creazione di un sistema di esportazione dei dati non attribuiva alle compagnie alcuna discrezionalità nella decisione circa la tipologia dei dati oggetto di trasferimento, né tantomeno in merito ai termini e alle modalità del trasferimento. In ogni caso i dati avrebbero dovuto essere trasmessi 72 ore prima della partenza e aggiornati al fine di garantirne l'esattezza.

9. Osservazioni critiche in merito al testo dell'accordo PNR

Come si è visto, il nuovo testo dell'accordo affrontava alcuni dei rilievi problematici delle precedenti versioni e che avevano formato oggetto di aspre polemiche da parte del Parlamento Europeo e degli altri organismi istituzionali comunitari deputati alla tutela dei dati personali.

In particolare, l'accordo riduceva i dati PNR richiesti da 34 a 19 . Tuttavia, secondo quanto osservato da attenta dottrina[521], questa riduzione del numero dei dati PNR era più teorica che pratica in quanto essa era frutto di una semplice fusione di rubriche di dati già esistenti piuttosto che una vera e propria riduzione del numero di dati richiesti[522]. All'atto pratico, infatti, nessuna tipologia di dato PNR sembrava essere stata realmente espunta dalla lista originaria.

Un secondo aspetto di critica da parte della dottrina riguardava il numero di autorità americane aventi accesso ai dati raccolti, che sotto l'impero dell'accordo del 2007 aveva subito un vistoso aumento[523]. Al di là del DHS, infatti, i dati PNR potevano essere diffusi a tutte le agenzie associate a quest'ultimo, ivi comprese la CIA e l'FBI. Inoltre, i dati PNR sarebbero stati suscettibili di trasferimento verso paesi terzi senza che fosse previsto almeno una consultazione preventiva delle

[520] Flavien MARIATTE Conclusion du nouvel accord UE/USA sur le transfert des données PNR Europe n° 10, Octobre 2007, comm. 247
[521] Loïc GRARD, nota 518
[522] Idem.
[523] Ibidem

autorità europee. Tale situazione suscitava le critiche del Presidente del Garante Europeo per la protezione dei dati Peter Hustinx[524] che osservava come "*there is no limitation to what U.S. authorities are allowed to do with" the data" and "[t]he absence of a robust legal mechanism that enables EU citizens to challenge the misuse of their personal information*."

Insomma, che l'accordo costituisse una compressione della privacy dei passeggeri europei non vi è era ombra di dubbio. Già nel caso Leander[525] la Corte di Strasburgo aveva evidenziato che la raccolta e la trasmissione di informazioni a carattere personale da parte di autorità pubbliche costituiva di per sé un'ingerenza ai sensi dell'art. 8 della CEDU.

Ma un diverso profilo di censura dell'accordo definitivo riguardava la durata di conservazione dei dati. La Corte di Strasburgo, nel caso Rotaru[526], aveva avuto modo di affermare che la conservazione di dati personali in un file doveva avvenire soltanto per un periodo di tempo limitato. La dottrina[527] non ha mancato di rilevare come detta durata fosse di tre anni e mezzo secondo l'accordo PNR del 2004 e come, detta durata, sotto l'impero dell'accordo PNR del 2007, fosse passata a 15 anni[528]. Il tutto sulla base di un termine che oltre ad essere di per sé eccessivamente ampio, era determinabile soltanto in funzione della discrezionalità delle competenti autorità USA. Infine, nessuna garanzia veniva fornita circa la distruzione dei dati non consultati[529].

Un ulteriore profilo di critica atteneva alla violazione, da parte dell'Accordo del 2007, del principio della finalità limitata, secondo cui i dati personali devono essere raccolti per fini determinati e legittimi e non possono essere utilizzati in modo incompatibile con detti fini. Orbene, ai sensi dell'accordo punto 1 lettera DHS le competenti autorità USA avrebbero potuto utilizzare i dati PNR esclusivamente per fini di prevenzione e repressione di terrorismo internazionale e crimini connessi ad altri gravi reati compresa la criminalità organizzata. Tuttavia, mentre la lotta al terrorismo era una finalità ampia ma dal contenuto determinabile, altrettanto non poteva dirsi in relazione alla categoria degli "altri gravi reati", posto che dalla disposizione in esame non era possibile evincere né di quali gravi reati si parlasse, né di quali fossero i parametri onde valutare detta gravità[530].

Tale previsione, conseguentemente, violava il principio della finalità limitata e la relativa violazione era resa ancor più evidente in considerazione del fatto che, oltre a dette finalità, i dati

[524] Letter from Peter Hustinx, European Data Protection Supervisor, to Wolfgang Schauble, Minister for the Interior (June 27, 2007), available at http://epic.org/privacy/pdf/hustinx-letter.pdf.
[525] Leander c. Svezia, sentenza del 26 marzo 1987 §§ 19-22, série A no 116, reperibile su reperibile su www.echr.coe.int
[526] Rotaru c. Romania, Sentenza del 4 maggio 2000 reperibile su www.echr.coe.int
[527] Flavien MARIATTE , nota 517
[528] Di cui sette anni in una banca dati attiva, otto anni in una banca dati dormiente, non operativa
[529] Cfr. Flavien MARIATTE, nota 517
[530] Cfr, Loïc GRARD, nota 520

PNR avrebbero potuto essere utilizzati "*in qualsiasi procedimento giudiziario penale o secondo quanto altrimenti previsto dalla legge*". In altre parole, forte era il sospetto che i dati PNR potessero finire con l'essere utilizzati in procedimenti penali che nulla avevano a che vedere con terrorismo e criminalità organizzata[531].

Anche la mancanza di solidi mezzi di ricorso in favore dei cittadini europei ha costituito un profilo rilevante di critica all'accordo del 2007. In particolare, in considerazione del punto 9 par. 2 dell'accordo PNR del 2007 dopo l'affermazione del principio per cui "*il presente accordo non intende derogare o apportare modifiche alle leggi degli Stati Uniti d'America o dell'Unione Europea o dei suoi Stati membri*" si soggiunge che esso "n*on crea né conferisce alcun diritto o beneficio ad altre persone o enti pubblici o privati"* [532].

In altri termini la rilevanza della lettera del DHS e delle garanzie ivi previste dal punto di vista degli interessati dal trattamento era pressoché nulla ed eventuali violazioni avrebbero potuto essere fatte valere ed avere conseguenze esclusivamente su di un piano politico nella misura i cui le competenti autorità comunitarie avessero lamentato il mancato rispetto degli impegni assunti dalle autorità USA e quindi delle norme attributive di diritti ai singoli[533].

Infatti, sebbene la lettera del DHS sostanzialmente si impegnasse a riconoscere ai cittadini europei i mezzi di ricorso di cui al Privacy Act del 1973, era pur vero che quest'ultimo strumento normativo non era invocabile da parte di cittadini di stati diversi dagli USA o, comunque, non residenti negli USA. Conseguentemente, diveniva lecito chiedersi se una decisione politica contenuta nella lettera del DHS fosse realmente in grado di estendere la tutela di uno strumento normativo e consentire così ai cittadini europei di beneficiare dei diritti di accesso, rettifica e di rimedio giurisdizionale[534].

L'accordo in esame, inoltre, non soddisfaceva le aspettative circa le garanzie apprestate a tutela dei dati sensibili. Sebbene questi ultimi risultassero espunti dalle 19 categorie di dati oggetto di trasmissione, deve sottolinearsi come alcune categorie quali le "osservazioni generali" nonché la cronistoria delle modifiche al PNR potevano comunque includere dati sensibili[535] . Invero, sebbene la lettera del DHS prevedeva che gli USA avrebbero fatto ricorso ad "un sistema automatizzato che filtra i codici e termini PNR sensibili" e che non utilizzava tali informazioni, ciò nondimeno il DHS se necessario avrebbe comunque potuto utilizzare dati sensibili contenuti nei PNR "in casi eccezionali in cui vi fosse pericolo o fosse seriamente minacciata la vita della persona interessata o

[531] Idem
[532] Ibidem
[533] Cfr. Alfredo Terrasi, nota 463
[534] Idem
[535] Marco Botta Mario Viola De Azevedo Cunha nota 1

di altre persone". [536] Come è stato osservato, il carattere troppo elastico di tale eccezione avrebbe potuto vanificare, sulla base di valutazioni completamente discrezionali della autorità USA, le già scarse garanzie previste nella lettera del DHS, configurando così una situazione difficilmente compatibile con il requisito delle garanzie appropriate di cui all'art. 6 della Convenzione 108[537].

Infine, l'accordo era criticabile perché le istituzioni comunitarie avevano sostanzialmente proceduto ad una svendita della tutela dei dati personali dei passeggeri in funzione di un accordo le cui finalità erano esclusivamente quelle di salvaguardare le esigenze di sicurezza degli USA e non anche quelle dell'Unione Europea. Dall'accordo PNR, infatti, l'Unione Europea non avrebbe ricavato nulla, neppure sotto il profilo della sicurezza[538].

Le osservazioni che precedono lasciavano presagire, pertanto, che il contenzioso internazionale sui PNR non si sarebbe affatto risolto con questo accordo, anzi ne giustificavano vieppiù la durata temporanea.

10. Il nuovo e recente accordo PNR 2012. Cenni

Come si è visto nelle pagine precedenti gli accordi PNR sono stati tutti stipulati per periodi di tempo determinati e soggetti a revisione periodica. L'ultimo accordo veniva a scadere nel 2012 e, pertanto, all'avvicinarsi del termine, vi era la necessità di pervenire alla stipula di un nuovo accordo al fine di permettere alle autorità americane di poter continuare ad accedere ai dati PNR delle compagnie aeree europee per finalità di contrasto della criminalità e di lotta al terrorismo.

Ciò premesso, nel frattempo era entrato in vigore il Trattato di Lisbona e con esso anche le disposizioni che conferivano al Parlamento Europeo un maggiore potere di incisione nell'ambito della procedura volta alla conclusione degli accordi internazionali. Invero, uno dei progressi maggiori apportato dal trattato di Lisbona è consistito non soltanto nell'aver semplificato considerevolmente la procedura di negoziazione e di conclusione degli accordi internazionali - segnatamente grazie alla fusione della Comunità Europea e dell'Unione Europea in una sola entità giuridica- ma di aver anche attribuito un potere di veto in capo al Parlamento Europeo (secondo quanto previsto dall'articolo 218 TFUE) per quanto riguarda gli accordi internazionali rientranti in quei campi in cui si applica la procedura legislativa ordinaria.

[536] Cfr. Punto 3 par. 4 dell'accordo
[537] Marco Botta Mario Viola De Azevedo Cunha, nota 1
[538] Idem

Tra questi, per effetto dell'abolizione del sistema a pilastri operata dal Trattato di Lisbona, figura oggi anche la cooperazione di polizia e giudiziaria in materia penale. Tale quadro normativo, dunque, avrebbe dovuto permettere al Parlamento di esercitare un controllo democratico rilevante sulla dimensione esterna di una materia in cui, nel contesto dell'architettura istituzionale previgente, non esercitava alcun ruolo significativo.

Proprio per questo motivo, alla luce del ruolo pressoché paritario del Parlamento rispetto al Consiglio nell'ambito della procedura volta alla conclusione di trattati internazionali sullo scambio dei PNR, i commentatori hanno atteso con molta curiosità di vedere in che modo l'istituzione democratica europea avrebbe fatto ricorso delle sue nuove prerogative al fine di influire sul contenuto del nuovo accordo[539].

Ciò premesso, i negoziati avviati dalla Commissione con la controparte statunitense nel gennaio del 2011 si sono conclusi nel dicembre del 2011, ed il nuovo accordo è stato firmato in data 14.12.2011 con entrata in vigore al 1 luglio 2012[540].

Il Parlamento Europeo, chiamato a pronunciarsi nell'aprile 2012 ha, contro ogni aspettativa, approvato l'accordo, e ciò nonostante il suo contenuto fosse stato in precedenza criticato da parte del Parlamento medesimo oltre che da parte del GEPD e del Gruppo di Lavoro ex art. 29 a causa delle violazioni manifeste degli standard europei in materia di protezioni dei diritti fondamentali.

La luce verde data dal Parlamento all'approvazione del testo ha colto di sorpresa la dottrina, la quale ha constatato come, ancora una volta, le motivazioni politiche e diplomatiche abbiano prevalso sulle preoccupazioni relative alla protezione dei diritti fondamentali[541]. In particolare, secondo alcuni commentatori le autorità americane avrebbero persino ventilato la possibilità di revocare l'esenzione dal visto per l'ingresso negli Stati Uniti prevista a favore dei cittadini della maggior parte dei Paesi membri dell'Unione Europea[542].

Innanzitutto l'accordo prevede che i dati siano raccolti per finalità di lotta al terrorismo ed alla grande criminalità transnazionale[543]. Tuttavia, ad avviso della dottrina, la formulazione dell'articolo 4 dell'accordo risulta eccessivamente estesa e vaga, aprendo così le porte ad un'estensione inammissibile delle finalità. Sotto questo profilo la dottrina si chiede se le zone d'ombra create dalle disposizioni di questo accordo potranno in alcun modo consentire l'utilizzo di questi dati per finalità

[539] Loïc GRARD Nouvelle actualité des accords PNR . - Sûreté du transport aérien contre sécurité juridique Revue de droit des transports n° 3, Juillet 2012, repère 3
[540] Cfr. GUUE n. L. 174 4 luglio 2012
[541] Sylvie PEYROU *Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne* » in Revue Europe n° 7, Juillet 2012, étude 8
[542] Idem
[543] Sylvie PEYROU, nota 541

diverse da quelle espressamente dichiarate, quali ad esempio la repressione delle violazioni delle leggi sull'immigrazione[544].

Inoltre, rispetto al vecchio accordo del 2004, nessun passo avanti è stato fatto con riferimento alla quantità di dati trasferiti. La riduzione delle 34 categorie di dati a 19 è soltanto apparente, e frutto di un mero accorpamento di categorie già esistenti[545].

Allo stesso modo, la durata di conservazione di dati appare eccessiva. Tale durata non è stata ridotta rispetto ai precedenti accordi ma, al contrario, ulteriormente allungata senza un reale bilanciamento. Invero, secondo i termini dell'accordo, i dati vengono inizialmente conservati in una banca dati attiva per un minimo di cinque anni per poi essere trasferiti in una banca dati "dormiente" per dieci anni supplementari. Dopo quindici anni, dunque, i dati così conservati vengono resi completamente anonimi ed in tal caso il loro periodo di conservazione non conosce alcun limite[546]. Tuttavia, l'accordo prevede che questi dati anonimi possano, in qualsiasi momento, essere "ri-personalizzati" nell'ambito di indagini da parte delle competenti autorità americane in relazione a rischi concreti per la sicurezza nazionale ovvero in presenza di indizi relativi alla commissione di gravi reati[547].

Un piccolo progresso è stato raggiunto, invece, per quanto riguarda le modalità di trasferimento dei dati rispetto al precedente accordo del 2007, in quanto il nuovo accordo prevede oramai un trasferimento secondo la modalità "push". Allo stesso modo i cittadini dell'Unione Europea saranno avvisati dell'utilizzo dei loro dati PNR ed avranno ugualmente il diritto di accesso ai loro dati PNR al fine di ottenerne la rettifica o la cancellazione in caso di inesattezza.

L'accordo prevede ugualmente il diritto di ricorso amministrativo o giudiziario conformemente alla legge americana per i cittadini europei i cui dati siano stati utilizzati in maniera illecita.

La dottrina tuttavia lamenta l'inadeguatezza della tutela giurisdizionale prevista. Ad onta dei numerosi richiami alle leggi americane in materia di protezione della privacy contenute nel testo del nuovo accordo, la dottrina si chiede in che misura i diritti ivi menzionati possano essere azionati nella pratica. La questione si pone in maniera alquanto acuta in quanto il Privacy Act non è applicabile ai dati PNR. Se si aggiunge poi che l'art. 21 dell'accordo precisa che quest'ultimo "non *crea né conferisce in virtù del diritto degli USA alcun diritto o vantaggio su qualsiasi altra persona pubblica privata o entità*" insorgono seri dubbi circa l'effettività della tutela prevista. Sotto questo profilo è stato osservato che il diritto ad un ricorso efficace e all'accesso ad un tribunale imparziale in conformità con la Carta dei Diritti Fondamentali dell'Unione Europea è invece espressamente

[544] Cfr. Loïc GRARD 539
[545] Cfr. Sylvie PEYROU nota 541
[546] idem
[547] Ibidem

previsto nella decisione comportante l'accettazione dell'Unione dell'accordo PNR tra UE e Australia firmato a Bruxelles il 29 settembre 2011 ed entrato in vigore il 1 giugno 2012[548].

In definitiva, secondo la dottrina dominante, il nuovo accordo PNR si sostanzia in una violazione manifesta degli standard europei in materia di protezione dei diritti fondamentali[549]e, sotto questo profilo, l'approvazione del Parlamento configura un pericoloso precedente, posto che anche un certo numero di altri paesi sono interessati della cooperazione sui dati PNR come l'Arabia Saudita, il Giappone, Corea del Sud, il Qatar e la Russia[550].

In ogni caso, a parere di chi scrive, la decisione del Parlamento, seppur criticata sotto molti aspetti, richiede di essere contestualizzata in quanto, viste le circostanze del caso, un rigetto *de plano* dell'accordo poteva non essere l'opzione più saggia.

Infatti, l'assenza di un accordo a livello internazionale, non avrebbe certo impedito alle autorità americane di avviare dei negoziati bilaterali con ciascuno Stato membro, mettendo così in pericolo la coerenza del sistema. Inoltre, l'assenza di un'autorizzazione europea al trasferimento dei dati dei passeggeri degli aerei europei verso gli Stati Uniti non avrebbe in alcun modo ostacolato le autorità americane nell'ottenere comunque i dati PNR, atteso che tre dei quattro CRS esistenti a livello mondiale si trovano proprio sul suolo americano e sono, pertanto, soggetti alle leggi federali degli USA.

Sembra, dunque, che nel voto del Parlamento abbia prevalso un certo pragmatismo politico in nome della buona cooperazione transatlantica nella lotta contro il terrorismo.

[548] (GUUE n. L 186 14 luiglio 2012 p. 1)
[549] Idem
[550] Loïc GRARD , nota 539

PARTE QUARTA

L'ACCORDO SAFE HARBOUR

In dottrina è stato osservato come l'emanazione di una direttiva contenente delle disposizioni in materia di trasferimento all'estero dei dati personali - che ne determinano sostanzialmente l'applicazione extra-territoriale – rappresenti una dimostrazione tangibile del ruolo più determinato che l'Unione Europea ha iniziato a giocare sulla scena internazionale a seguito della maggiore integrazione dei suoi Stati membri[551].

Infatti, come si è visto nelle pagine precedenti, grazie all'emanazione della Direttiva 95/46/CE sulla protezione dei dati personali l'Unione Europea è riuscita gradualmente ad affermare, a livello internazionale, un modello propriamente europeo in materia di protezione dei dati. Si è, d'altronde, visto come a seguito della sua adozione, numerosi Stati terzi abbiano provveduto ad adeguare le proprie legislazioni nazionali al fine di ravvicinarle il più possibile allo standard di protezione elaborato a livello europeo nonché a dotarsi di specifiche legislazioni laddove ne fossero privi. E' il caso di paesi come il Canada, Israele, la Svizzera, l'Uruguay e l'Argentina.

Gli Stati Uniti, invece, pur essendo consapevoli del fatto che il loro approccio settoriale alla protezione dei dati personali non avrebbe mai incontrato l'approvazione dell'Unione Europea, non hanno provveduto a modificare la propria legislazione nazionale, obiettivo questo, peraltro irraggiungibile anche in considerazione del limitato periodo di tempo intercorrente tra l'entrata in vigore della direttiva e la sua trasposizione negli ordinamenti nazionali degli Stati membri, ossia poco più di due anni[552].

Questa situazione presentava dei rischi concreti di paralisi dei flussi di dati tra l'Unione europea e il continente americano, con l'immediata conseguenza di ostacolare gli scambi commerciali tra le due sponde dell'Atlantico, stimati, in quell'epoca in un volume di affari da 180 miliardi di dollari[553].

Infatti, il mancato rispetto della Direttiva avrebbe implicato che, in un'era tecnologica come quella attuale, non vi sarebbero state più transazioni bancarie transatlantiche,

[551] Barbara Crulchfield; Patricia Lynch; Susan J. Marsnik, nota 288

[552] Patrick E. Cole, "New challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws" in 17 N.Y.U J. INT'L L. & POL. 893, 897-98 (1995)

[553] Dorothée Heisenberg, nota 6

prenotazioni aeree o alberghiere e nessun acquisto tramite carte di credito europee[554]. Sotto questo profilo basti pensare che, ogni giorno, milioni di persone nell'Unione Europea accedono a siti Internet di proprietà o comunque riconducibili ad imprese o organizzazioni site negli Stati Uniti, ove vengono caricati giornalmente migliaia di dati, ed ove vengono realizzati innumerevoli accessi a conti correnti bancari e pagamenti con carte di credito. In tal modo, i dati personali relativi a milioni di utenti lasciano inesorabilmente il territorio dell'Unione europea e quindi la giurisdizione della medesima, per essere trasferiti verso gli Stati Uniti.

Di pari passo, le imprese americane avrebbero anche incontrato dei seri ostacoli nella gestione dei loro nove milioni di dipendenti europei[555]. Alla luce delle ragioni fin qui esposte, dunque, la disputa tra Stati Uniti ed Unione Europea in merito all'applicazione extraterritoriale della Direttiva avrebbe potuto, con ogni probabilità, cagionare un vero e proprio embargo sui flussi intercontinentali di dati suscettibile di degenerare in una vera e propria guerra commerciale su scala internazionale[556].

Nel 1998, pertanto, il US Department of Commerce e la Commissione Europea iniziarono ad intavolare negoziati durati due anni al fine di raggiungere una soluzione di compromesso[557].

Questi negoziati si sono conclusi mediante la finalizzazione di un accordo in data 27 Luglio 2000 che prese il nome di "Safe Harbor". Successivamente la Commissione Europea approvava formalmente i principi del Safe Harbor, con data effettiva al 1 novembre 2000[558].

Il Parlamento Europeo, che all'epoca era soltanto consultato e non aveva alcun potere di impedire la conclusione dell'accordo o di influire sul suo contenuto, esprimeva parere contrario alla decisione di adeguatezza in ragione di una complessa combinazione di fattori sostanziali, procedurali e politici e chiedeva una revisione del testo[559].

---

[554] Mike France, "*Once again, technology is outrunning privacy law*" in Business Week Online, Mar. 13 2000 at http://www.businessweek.com/technology/content/003/ep0313.htm aggiornato al 14.02.2013

[555] David Aaron, "Privacy across the pond", Star Trib., June 4, 2000 at 11D.

[556] Kevin Bloss, "Raing or Razing the e-curtain" The EU directive on the protection of personal data", 9 Minn. J. Global Trade 645, 654 655 (2000)

[557] idem

[558] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce in GUUE L 215 25/08/2000 p. 0007-00047

[559] European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS)), consultabile su http://epic.org/privacy/intl/EP_SH_resolution_0700.html

Il programma Safe Harbour é stato concepito al fine di conciliare le difformità tra la normativa americana e quella europea in materia di protezione dei dati personali. Si tratta, dunque, di una soluzione di compromesso in quanto il programma è diretto a porre in qualche modo rimedio alle inadeguatezze segnalate dall'Unione Europea nella legislazione americana in materia di protezione dei dati personali, senza richiedere un particolare intervento legislativo sul punto[560]. L'accordo entra in gioco ogniqualvolta dati personali protetti dalla Direttiva vengono trasferiti ad una società o ad un'impresa americana.

L'adesione al Safe Harbor, infatti, crea la presunzione che l'organizzazione aderente fornisce un adeguato livello di protezione dei dati personali abilitandola, così, a ricevere i dati da parte degli Stati Membri dell'Unione Europea senza incorrere nel rischio di sanzioni (da qui il termine Safe Harbor cioè "approdo sicuro") da parte delle autorità garanti degli Stati UE.

L'adesione al Safe Harbor è assolutamente facoltativa, le imprese americane non sono obbligate ad aderire al programma, ben potendo optare di ottenere direttamente l'autorizzazione al trasferimento dei dati presso le competenti autorità garanti degli Stati membri, segnatamente mediante l'utilizzo di garanzie contrattuali o di codici di condotta. In ogni caso, se un'impresa sceglie di aderire al Safe Harbor, l'approvazione da parte degli Stati membri è presunta, sebbene permanga l'obbligo in capo all'azienda aderente di notificare all'autorità garante dello Stato membro competente l'operazione di trasferimento di dati.

E' stato osservato in dottrina che il Safe Harbor non sarebbe né un trattato, né un accordo internazionale, ma come lo stesso sarebbe il prodotto di due azioni unilaterali: i principi di matrice Usa e la decisione di adeguatezza emessa dalla Commissione[561]. Ciò significa che la decisione sull'adeguatezza formulata dalla Commissione Europea potrebbe essere revocata nel caso in cui l'accordo non funzionasse come dovrebbe. Allo stesso modo, è stato osservato come il Safe Harbor presenti un carattere ibrido, in quanto è il prodotto di un mix tra la self regulation di tradizione americana e il controllo amministrativo da parte di un ente statale come da tradizione europea consolidata.[562]

[560] Wiliam J Long, Marc Pang Quek "Personal data privacy protection in an age of globalization: the UE-EU safe harbor compromise", in Journalof European Public Policy :3 June 2002 325-344.
[561] StephenJ. Kobrin "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territoriale jurisdiction and global governance" in Review of International studies (2004), 30, 11-131
[562] Dorothe Heisenberg, nota 6 p. 74

L'accordo Safe Harbor è costituito, oltre che dai Principles, anche da un set di domande frequenti ("frequently asked questions" o "FAQ") che contengono una sorta di glossa elaborata a cura del Department of Commerce e diretta a fornire maggiori informazioni circa il significato dei Principi. Inoltre, esso contiene una panoramica di come gli impegni assunti dall'impresa aderente verranno rispettati negli Stati Uniti, nonché un memorandum sulle azioni risarcitorie messe a disposizione degli individui.

L'adesione al Safe Harbor avviene su base auto-certificativa. L'Autocertificazione avviene mediante invio di una lettera da parte della società o dell'impresa al Department of Commerce in cui si dice che l'impresa aderisce al Safe Harbor oppure attraverso la registrazione online sul sito del Department medesimo. La lettera deve includere informazioni specifiche quali i contatti ed una descrizione di ciò che l'impresa fa con rispetto ai dati personali ricevuti dalla UE. L'autocertificazione deve includere una descrizione della privacy policy dell'azienda, inclusi dettagli circa il luogo in cui tale policy è consultabile da parte del pubblico, la sua data di vigenza e il nome del contatto che gestisce le lamentele e le richieste di accesso alle informazioni.

Al fine di rispettare le regole stabilite dal programma Safe Harbor l'impresa deve inserirsi in un programma privacy che includa efficaci meccanismi di rispetto quali TRUSTe e BBB Online seal program o sviluppare delle proprie politiche privacy in conformità con i Principi o auto-certificare al Department of Commerce che la società è già soggetta a una specifica legge o regolamento di settore o i impegna ad aderire ai Principi in contratti con parti che trasferiscono dati dall'UE in conformità con le clausole standard approvate dalla UE. I programmi TRUSTe e BBBOnline prevedono infatti un "sigillo di approvazione" da parte di un ente terzo privato che viene conferito ai web sites che rispettano gli standard del comparto industriale di appartenenza in materia di protezione della privacy[563]. Allo stesso modo detti programmi offrono dei meccanismi di "ADR" (alternative dispute resolution) per i ricorsi dei consumatori. Il meccanismo di tutela nell'ambito del Safe Harbor si basa infatti sui ricorsi. Inizialmente i ricorsi sono gestiti da meccanismi di ADR da parte dei privacy seals programs ovvero dalle autorità garanti UE. Se le imprese aderenti non rispettano la decisione ADR, allora la Federal Trade Commission o il Department of Transportation (in funzione dell'agenzia competente per settore di riferimento) possono imporre delle sanzioni. Le violazioni più gravi possono essere sanzionate con la cancellazione dalla lista degli aderenti al Safe Harbor e con lo interruzione dei flussi di dati da e verso la UE.

[563] Idem

I benefici del Safe Harbor derivano dalla data in cui l'impresa auto-certifica l'adesione al Department of Commerce la sua adesione al Safe Harbor .

In linea di massima il Principi Safe Harbor ricalcano quelli della Direttiva.

In primo luogo è previsto il *principle of notice*. L'impresa deve cioè informare gli individui circa gli scopi per i quali i dati vengono raccolti e le modalità del loro utilizzo. Inoltre le imprese devono spiegare le modalità di presentazione dei ricorsi, i tipi di soggetti terzi ai quali i dati possono essere comunicati e le possibilità per i soggetti interessati di limitare tale comunicazione. Le informazioni devono essere presentate in "*a clear and conspicuos language"* nel momento stesso in cui gli individui sono richiesti di fornire le proprie informazioni o subito dopo, ma le informazioni devono essere fornite prima che l'impresa utilizzi l'informazione per scopi diversi da quelli per cui esse erano stati raccolti o li comunichi a soggetti terzi.

In secondo luogo è previsto il *principle of choice*, secondo cui l'impresa deve fornire gli individui la possibilità di decidere secondo un criterio di "*opt out*" se le proprie informazioni personali possono essere comunicate a soggetti terzi o essere utilizzate per scopi diversi da quello preventivamente autorizzato. Inoltre, per quanto riguarda i dati sensibili, il soggetto interessato deve necessariamente fare "*opt in*" prima che tale informazioni possano essere comunicate a soggetti terzi o usati per uno scopo alternativo.

Il *principle of onward trasfer* si applica ove l'impresa che ha raccolto i dati intenda comunicarli ad un soggetto terzo. Ai sensi del Safe Harbor, infatti, l'impresa può comunicare i dati raccolti ad un soggetto terzo che agisca quale suo agente dopo aver verificato che il soggetto terzo rispetti i requisiti del Safe Harbor o della Direttiva Dati ovvero altra adeguata misura di protezione dei dati. Alternativamente l'impresa potrà stipulare un accordo scritto con il soggetto terzo che garantisca che il destinatario dei dati offra "almeno il medesimo livello" di protezione dei dati previsto dal Safe Harbor.

Secondo il *Principle of security,* invece, le imprese aderenti al Safe Harbor dovranno "adottare precauzioni ragionevoli" in ordine a "perdita,utilizzo improprio e accesso non autorizzato, comunicazione, alterazione e distruzione" dei dati.

Il quinto principio riguarda la "*Data Integrity*", e prevede che i dati personali raccolti debbano essere pertinenti rispetto allo scopo specifico della loro raccolta. Ciò significa che l'impresa non potrà effettuare un trattamento dei dati difforme o incompatibile con gli scopi per i quali i dati sono stati raccolti.

Il *Principle of access* implica invece il diritto di accesso da parte del soggetto interessato ai dati personali che lo riguardano al fine di correggere, rettificare o cancellare

i dati non accurati. Tuttavia, se il costo in termini di tempo e di denaro per l'impresa fosse sproporzionato rispetto al rischio, questa non sarà obbligata a fornire detto accesso.

Il principio finale è quello di *Enforcement*. Affinché la protezione dei dati possa essere considerata efficace le imprese aderenti al Safe Harbor dovranno approntare dei meccanismi efficaci di ricorso per i soggetti interessati e rendere chiare le conseguenze in caso di violazione dei principi. Le misure attuate dalle imprese devono quantomeno includere "mezzi di ricorso prontamente disponibili, abbordabili ed indipendenti" che permettano alla lamentela del soggetto di essere indagata e risolta in conformità ai Principi inclusi risarcimento del danno se applicabile. Inoltre vi dovrebbero essere procedure di "follow up" al fine di verificare che l'impresa stia effettivamente rispettando i Principles.

La Federal Trade Commission mantiene una lista di enti aderenti al Safe Harbor sul proprio sito web. La violazione degli accordi Safe Harbor potrebbe essere sanzionata ai sensi della Sezione 5 del Federal Trade Commission Act, o del Titolo 49 della Sezione 5 del US Code da parte dell'autorità del Department of Transportation[564]

Deve notarsi che la decisione di aderire ai Safe Harbor Principles implica che i dati trasferiti allorquando l'impresa godeva dei benefici Safe Harbor continueranno ad essere protetti dal Safe Harbors anche qualora successivamente l'impresa esca dal programma.

Secondo il sito governativo del Department of Commerce l'adesione al Safe Harbor presenta molteplici vantaggi in quanto fornisce alle imprese americane la possibilità di rispettare la direttiva 95/46/CE in maniera semplice e senza dover sostenere costi irragionevoli[565]. Invero, firmando tale accordo un'impresa certifica ai clienti europei delle organizzazioni europee che essa fornisce adeguata protezione della privacy dei dati personali secondo i termini della direttiva. La protezione fornita dall'impresa verrà considerata adeguata semplicemente in virtù della sua partecipazione all'accordo e trasferimenti di dati personali all'impresa continueranno ininterrotti. Se uno Stato membro richiede l'approvazione preventiva di trasferimenti di dati, i requisiti " saranno denunciati ovvero approvati automaticamente" nei confronti di una impresa statunitense facente parte del the Safe Harbor.

Aderire Safe Harbor inoltre consente ad una impresa americana di evitare negoziati con le autorità di protezione dei dati di ciascuno Stato membro nel quale esercita la

[564] Wiliam J Long, Marc Pang Quek, nota 560

[565] U.S.-EU Safe Harbor Overview consultabile su http://export.gov/safeharbor/eu/eg_main_018476.asp

propria attività. Aderire è semplice può essere effettuato attraverso il sito Internet della the Commerce Department's.

Ferme restando le suesposte considerazioni in termini di vantaggi per le imprese, il Safe Harbor è stato aspramente criticato da parte della dottrina. In primo luogo la creazione del Safe Harbor è il frutto evidente di un compromesso e, come tutti i compromessi, esso non risulta gradito a nessuna delle due parti all'accordo. Invero, è stato notato come il Safe Harbor costituisca un interfaccia tra il sistema Europeo di regolamentazione formale della privacy e il sistema americano di self regulation, i quali sono qualitativamente differenti l'uno dall'altro[566].

In secondo luogo il Safe Harbor è stato criticato anche in quanto pochissime imprese USA vi hanno aderito e ciò soprattutto in considerazione del fatto che non è previsto alcun obbligo di adesione. Un mese dopo la sua istituzione, infatti, soltanto tre società avevano presentato domanda di adesione. Il numero di società registrate aumentava a trenta dopo sei mesi dalla sua entrata in vigore[567]. Alla data del 7 maggio 2003, soltanto 338 imprese avevano aderito, tra cui poche multinazionali[568]. Ciò, sempre a parere della dottrina, testimonierebbe come le sanzioni in caso di non compliance con gli standard europei in materia di privacy non siano particolarmente avvertite da parte delle imprese americane.

Allo stesso modo è stato notato come molte imprese americane ritengano troppo costoso attuare un programma complicato come il Safe Harbor, che potrebbe peraltro esporle ad imprecisate forme di responsabilità in Europa[569].

Inoltre, parte della dottrina ha altresì evidenziato il fatto che,oltre a conservare la lista delle imprese aderenti, non vi è nessun controllo da parte del Department of Commerce circa l'adeguatezza della privacy policy delle imprese aderenti o circa il rispetto, da parte delle medesime imprese, dello loro privacy policies[570]. Inoltre il Department of Commerce non garantisce l'accuratezza della lista e non si assume alcuna responsabilità per l'erronea inclusione, omissione o cancellazione di qualsiasi impresa, o di qualsiasi

[566] Stephen J Kobrin, 561
[567] Wiliam J Long, Marc Pang Quek, nota 560
[568] la lista delle società e delle imprese aderenti è consultabile all'indirizzo www.export.gov./sh_overview.html /safeharbor
[569] Juliana Gruenwald "Safe Harbor stormy waters", Interactive Week (30 ottobre 2000) disponibile su http://www.zdnet.com/zdnn
[570] Bell-Eder, Britney D.; Rynerson, Stephen D.; Soma, John T. "An analysis of the bilateral agreements between transnational trading groups: the US/EU E-commerce privacy Safe Harbor" in Texas International Law Journal 39 no 2 171-214 Wint 2004

azione relativa alla conservazione della lista[571]. L'unico reale controllo si verifica nel caso di una lamentale da parte di un soggetto secondo cui i termini e le condizioni del Safe Harbor non sono state adeguatamente rispettate, nel qual caso l'impresa potrebbe essere soggetta ad un'azione da parte della Federal Trade Commission o del Department of Transportation "for unfair or deceptive trade practices"[572]. In quest'ottica è stato osservato come a due anni dalla ratifica dell'accordo nessuna società americana era stata oggetto di sanzioni da parte della Federal Trade Commission per violazione delle disposizioni dell'accordo[573].

Fermo restando quanto ora esposto, il Safe Harbor presta altresì il fianco alle critiche di quella parte dei commentatori che ritiene dubbia la possibilità che la Federal Trade Commission o il Department of Transportation abbiano reale giurisdizione in merito ai casi di violazione dei principi, il che mette in discussione l'esistenza di un reale meccanismo di enforcement del Safe Harbor[574]. Invero, sebbene la giurisdizione della Federal Trade Commission sia stata estesa al commercio estero nel1952, ciò è avvenuto in maniera limitata, soltanto con rispetto alla giurisdizione sui monopoli stranieri. Quando nel 1975 il Congresso espandeva tale giurisdizione al fine di coprire le transazioni dei consumatori che influivano sul commercio, non ha mai specificamente incluso alcun riferimento alle transazioni straniere di consumatori stranieri. Onde per cui rimane dubbio il fatto che la Federal Trade Commission abbia giurisdizione nei confronti delle imprese americane che violano i principi Safe Harbor[575].

Allo stesso modo, il Safe Harbor è stato criticato in quanto non costituisce un passo in avanti per l'adozione, da parte degli USA di una normativa generale in materia di protezione dei dati (di cui costituirebbe al contrario un debole surrogato), con conseguente abbandono del tradizionale approccio basato sulla self regulation[576]. Sotto questo profilo, David Aaron, sotto segretario al commercio in seno al Department of Commerce dichiarava in occasione di un incontro con le imprese americane che "*these safe harbor principles have been developed and are aimed at a specificc situation – reassuring the Europeans that their privacy… will be protected…In no way does the US*

[571] Idem
[572] Ibidem
[573] Bell-Eder, Britney D.; Rynerson, Stephen D.; Soma, John T, ota 570
[574] John Graubert e Jill Coleman, "Consumer Protection and Antitrust Enforcement at the speed of light: the FTC meets the internet" in 25 Can-US L.J. 275-275 (1999)
[575] Julia Gladstone "The US Privacy balance and the European privacy directive: reflections on the United States Privacy Policy", Willamette J.Int'l L. & Dispute Res. 10, 10 (2000)
[576] Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717 (2001)

government intend for these safe harbor principles to be seen as precedents for any future changes in the US privacy regime"[577].

L'accordo ha raggiunto un momento di notorietà nel giugno 2001 quando la Microsoft ha aderito al programma a seguito della condanna al pagamento della multa in Spagna. Altre imprese come Dun & Beradstreet hanno aderito principalmente perché la Svezia aveva tagliato un trasferimento trans atlantico di dati. Data la sporadicità delle azioni dirette a garantire il rispetto dei termini dell'accordo, molte società sono state tentate dall'ignorare la direttiva sperando che le azioni verranno dirette soltanto a casi eclatanti o grandi imprese.

[577] David Aaron, Remarks before the Information Technology Session of America, Fourth Annual IT policy Summit.

CONCLUSIONI

I risultati della ricerca condotta nell'arco di questi tre anni di dottorato, così come illustrati nelle pagine che precedono, consentono di pervenire ad alcune importanti conclusioni che si procederà a rassegnare in questa sede.

Preliminarmente, l'analisi fin qui esposta ha, anzitutto, permesso di constatare come, in conformità con l'esperienza storica e con la tradizione giuridica di molti dei suoi Stati membri, anche per l'Unione Europea la protezione dei dati personali costituisce un vero e proprio diritto fondamentale dell'individuo.

In un vecchio continente memore dello scempio dei regimi totalitari - sotto l'impero dei quali i dati personali hanno subito una manipolazione costante e sistematica in chiave repressiva - l'esigenza di protezione degli individui contro le ingerenze nella loro privacy riacquista, oggi, significato in funzione della difesa della sfera privata dalle forme di controllo esercitate dalle nuove tecnologie. Il tutto pur sempre in chiave di antidoto allo Stato totalitario e come barriera contro eventuali nuove forme di schiavitù.

Si è visto, in particolar modo, come tale concezione, tipicamente europea, sia tributaria dell'esperienza del Consiglio d'Europa e della giurisprudenza della Corte Europea dei Diritti dell'Uomo. Il diritto alla tutela dei dati personali nasce, così, inizialmente in via pretoria per poi successivamente confluire all'interno delle disposizioni della Direttiva 95/46/CE. Da ultimo, lo stesso è stato formalmente "consacrato" all'interno di una disposizione *ad hoc* della Carta dei Diritti Fondamentali dell'Unione Europea (art. 8), alla quale il Trattato di Lisbona ha conferito valore vincolante, elevandola a parità di rango con gli altri trattati.

Come si è visto, inoltre, la visione europea della tutela dei dati personali quale patrimonio fondamentale dell'individuo contraddistingue il diritto europeo rispetto alle tradizioni giuridiche delle altre democrazie occidentali quali, segnatamente, gli Stati Uniti d'America, ed è foriera di vistose conseguenze anche sul piano della tutela legislativa.

Mentre in Europa, infatti, la tutela dei dati personali viene assicurata per mezzo di un quadro normativo generale ed uniforme viceversa, negli USA, ove la Costituzione federale non contempla espressamente la tutela dei dati personali nella rosa dei diritti costituzionali, quest'ultima viene approntata sulla base di una normativa altamente settoriale e frammentata, con evidenti discrasie tra il settore pubblico (generalmente regolamentato) e il settore privato, ove tradizionalmente vige un sistema di *self-regulation.*

Allo stesso modo, mentre negli USA la tutela contro le violazioni dei principi in materia di protezione dei dati personali viene generalmente realizzata attribuendo all'individuo la facoltà di esperire un'azione meramente risarcitoria al contrario, in Europa, la tutela dei dati è soggetta a un meccanismo di protezione multi-livello che caratterizza, d'altronde, il meccanismo di protezione europea di tutti i diritti fondamentali.

Invero, oltre alla possibilità di esperire un'azione risarcitoria dinanzi ad un giudice, la normativa europea ha approntato anche una tutela amministrativa, prevedendo l'istituzione, sul territorio di ciascuno Stato membro, di autorità garanti indipendenti dal potere politico dotate, oltre che di poteri di indagine e di monitoraggio delle misure nazionali di attuazione della normativa sovranazionale, anche del compito di conoscere dei ricorsi individuali da parte degli individui che lamentano la violazione dei propri diritti, nonché del potere di infliggere sanzioni nei confronti degli autori di dette violazioni.

Ciò premesso, l'analisi fin qui condotta ha permesso, altresì, di appurare l'esistenza di una vera e propria dimensione esterna del diritto dell'Unione Europea nella tutela dei dati personali, la quale costituisce, oltre che un corollario del carattere fondamentale di questo diritto, anche una risposta all'esigenza di proteggere i dati che fuoriescono dal territorio dell'Unione, quale conseguenza naturale ed inevitabile delle transazioni commerciali internazionali, nonché dell'intrecciarsi delle relazioni interpersonali nell'era di internet.

Si è, dunque, descritto quali sono i principi che governano la legittimità, ai sensi del diritto europeo, dei trasferimenti dei dati personali verso Paesi Terzi e si sono analizzati gli strumenti normativi di cui l'Unione Europea dispone in questo campo, ed in particolar modo l'utilizzo delle clausole contrattuali ovvero il ricorso agli accordi internazionali. Il tutto nell'ottica di garantire ai dati personali oggetto del trasferimento un adeguato livello di protezione. Per questo motivo, sempre su questo versante, si è avuto modo di rilevare la nascita di quella che è stata definita come una vera e propria politica estera legislativa dell'Unione Europea, volta ad assicurare, nell'ambito dei rapporti internazionali con gli Stati terzi, un elevato standard di protezione dei dati.

La complessa vicenda relativa al trasferimento dei dati PNR ha avuto il pregio di aver messo a nudo i problemi e le difficoltà relativi alla dimensione esterna della protezione dei dati personali e di aver rappresentato, sotto molti aspetti, la più efficace cartina di tornasole al fine di misurare i risultati conseguiti dalla politica europea in questa delicata materia.

Come è stato osservato dalla stessa Commissione durante la causa innanzi alla Corte di Giustizia, la vicenda del contenzioso sui PNR ha costituito, *prima facie*, un conflitto di leggi a livello internazionale, che ha permesso di cogliere appieno la portata della diversa concezione della tutela dei dati personali nelle tradizioni giuridiche europea ed americana, nonché le conseguenze

che tale diversa concezione è suscettibile di provocare. Infatti, nelle vicende PNR e SWIFT si assiste, prima di tutto, ad un vero e proprio scontro, sul terreno della protezione dei dati personali, tra due culture giuridiche molto distinte tra loro.

In secondo luogo, la vicenda dei PNR e dello SWIFT dimostra come sia importante per gli Stati membri dell'Unione Europea mantenere alta la guardia nella tutela dei diritti fondamentali in un'era, come quella attuale ove, sotto la minaccia costante del terrorismo internazionale e sulla scorta dell'imperativo della sicurezza, si assiste alla continua emanazione di leggi che, nell'obiettivo dichiarato di proteggere i cittadini e la democrazia, restringono le libertà fondamentali col rischio concreto di annientarle. E' innegabile sotto questo profilo che, a seguito degli attacchi dell'11 Settembre 2001 negli Stati Uniti a cui hanno fatto eco gli attentati di Madrid e di Londra, l'esigenza di rafforzamento della sicurezza nazionale ha influenzato, oltre che gli USA, anche le legislazioni di numerosi stati membri dell'Unione Europea.

Invero, è alquanto imbarazzante constatare la facilità con la quale, nel caso PNR, gli USA siano stati in grado di ottenere tutto quanto richiesto dalla loro legislazione interna senza scendere ad alcun compromesso con gli standard previsti dal sistema europeo[578]. E ciò nell'ottica di una relazione transatlantica che sembra troppo spesso frutto di unilateralismo piuttosto che di un vero dialogo tra potenze alleate. I negoziati hanno visto a più riprese, infatti, una Commissione sostanzialmente inerte nel recepire praticamente tutte le richieste provenienti dall'altra sponda dell'Atlantico, con un Consiglio che, da un lato, premeva per il loro accoglimento ed un Parlamento Europeo che, privo di qualsiasi potere di incidere concretamente sul contenuto degli accordi, è stato relegato all'impotente ruolo di Cassandra.

La situazione ora descritta risulta vieppiù sorprendente se si considera che questi ripetuti "cedimenti" da parte dell'Unione Europea sul terreno dei diritti fondamentali sono avvenuti in funzione di un accordo che avrebbe garantito esclusivamente la sicurezza degli USA ed in relazione al quale l'Unione Europea non ci avrebbe guadagnato nulla!

A ciò deve aggiungersi che, in realtà, gli USA raccolgono i dati PNR delle compagnie aeree europee sin da prima del 11 settembre 2001 e ciò senza alcun accordo. Sotto questo profilo la concatenazione di trattati PNR post 11 settembre che si sono susseguiti è servita soltanto ad ampliare ed a legittimare le pratiche di raccolta dei dati da parte delle agenzie federali USA. Dal canto suo, invece, l'annullamento dell'accordo da parte della Corte di Giustizia è stato definito in dottrina come una "vittoria di Pirro"[579] del Parlamento in quanto tale sentenza ha permesso la

[578] Rasmussen, D. Richard, nota 407

[579] Valentina Bazzocchi "*L'Accord entre l'Union européenne et les États Unis sur les données PNR*" consultabile su http://www.europeanrights.eu/index.php?funzione=A&op=5

conclusioni di un nuovo accordo in cui veniva contemplato un ulteriore ampliamento dell'autorità degli USA in questo campo[580].

In altri termini, le negoziazioni sul trasferimento del PNR hanno rappresentato un chiaro esempio in cui l'esigenza di sicurezza della collettività ha prevalso via via sul rispetto dei diritto fondamentali dei passeggeri in volo verso gli Stati Uniti.

L'avvento dell'amministrazione Obama, sotto questo profilo, ha cambiato sensibilmente le cose. Il cambio di rotta della politica americana, così come confermato anche in occasione del secondo discorso di inaugurazione del Presidente americano sembra denotare una maggiore consapevolezza del fatto che la protezione della sicurezza nazionale non richiede necessariamente come contropartita una rinuncia alla tutela dei diritti fondamentali, così come "il *mantenimento.. di una pace duratura non richiede uno stato di guerra perpetua*"[581]. Alla luce di queste considerazioni il Presidente Obama ha ritenuto di optare per una lotta al terrorismo basata, sul rafforzamento delle relazioni e della cooperazione con i paesi alleati, più che su di un ruolo unilaterale di polizia universale.[582].

Anche il nuovo Segretario del DHS Janet Napolitano ha espresso parole concilianti in relazione ad una revisione dell'accordo PNR con la UE affermando che "*The United States is committed to working closely with our European partners to develop innovative and effective ways to ensure our mutual safety while protecting the privacy and civil liberties of all citizens*"[583], a testimonianza della minore intransigenza dell'attuale amministrazione statunitense sui temi della sicurezza nazionale.

Ciò premesso, vicende come il contenzioso sui PNR o sullo SWIFT hanno, inoltre, dimostrato inequivocabilmente tutta la debolezza, sotto il profilo della tutela dei dati personali, della previgente struttura a pilastri dell'Unione Europea. Invero, se già il primo accordo PNR era stato criticato dal Parlamento Europeo, sulla scorta delle preoccupazioni riguardanti lo scarso livello di protezione della privacy individuale, l'annullamento di tale prima versione per effetto della decisione della Corte di Giustizia e la successiva conclusione di uno strumento interamente basato sul terzo pilastro ha permesso sostanzialmente di pervenire ad un testo in cui le garanzie a tutela dei dati personali risultavano assai più ridotte rispetto alla sua versione originaria. Inutile dire, infatti, che la negoziazione, anche del nuovo accordo 2007 sulla base di una decisione del Consiglio nell'ambito del terzo pilastro non giustifica un rilassamento nella tutela dei diritti fondamentali[584].

[580] Idem
[581] Obama Inauguration Speech 2013 Transcript Full Text
http://www.classicalite.com/articles/1090/20130121/obama-inauguration-speech-2013-transcript-full-text-read.htm
[582] Idem.
[583] Readout of Secretary Napolitano's Meetings with European Counterparts in Washington
http://www.dhs.gov/news/2010/12/09/readout-secretary-napolitanos-meetings-european-counterparts-washington
[584] Marco Botta Mario Viola De Azevedo Cunha, nota 1

Ciò ha permesso, altresì, di creare un pericoloso precedente, posto che la Commissione ed il Consiglio avrebbero avuto, anche con riferimento ai successivi accordi con il Canada, l'Australia ed il Giappone, la possibilità di fare ricorso ad una base giuridica che conferiva loro carta bianca per negoziare accordi in questa materia senza doversi confrontare con le istanze del Parlamento Europeo, né tantomeno fare i conti con il sindacato giurisdizionale della Corte di Giustizia.

L'entrata in vigore di Lisbona il 1 dicembre 2009 ha abolito la struttura a pilastri che caratterizzava l'assetto istituzionale previgente, spianando così la strada ad un coinvolgimento del Parlamento Europeo su di un piano paritario con il Consiglio nella conclusione degli accordi internazionali e, quindi, ad una sua maggiore capacità di incidere sul contenuto degli accordi medesimi. Come si è visto, tuttavia, la recente ed inspiegabile approvazione, da parte del Parlamento Europeo, del nuovo testo dell'accordo, dimostra ancora una volta come le ragioni della sicurezza e le pressioni della politica internazionale possano facilmente avere la meglio sulle esigenze di tutela dei diritti fondamentali.

In ogni caso, fermo restando il summenzionato incidente di percorso, il Trattato di Lisbona prevede gli strumenti necessari affinché la tutela dei dati personali divenga un'attività centrale dell'Unione Europea. Invero, sulla base dell'art. 87 TFUE è già previsto che il Parlamento e Consiglio adotteranno sulla base della procedura legislativa ordinaria le misure riguardanti la raccolta l'archiviazioni ed il trattamento e l'analisi e lo scambio di informazioni tra le autorità di polizia dei paesi membri. La procedura legislativa ordinaria che sostituisce quella di codecisione diviene lo strumento esclusivo legislativo per regolamentare anche le materie afferenti all'area dell'ex. Terzo pilastro, ossia la cooperazione tra le autorità giudiziarie e di polizia in materia penale. Pertanto, tenuto conto del nuovo potere di veto del Parlamento oggi l'Unione dovrà tenere in maggiore conto l'opinione di quest'ultimo.

In ogni caso, nell'ambito di queste conclusioni non si possono tacere i risultati che la politica estera legislativa dell'Unione Europea è riuscita a conseguire nel campo della tutela dei dati personali. Invero, come si è detto profusamente nelle pagine che precedono, già soltanto l'emanazione della direttiva 95/46/CE ha innescato un meccanismo di risposta a livello internazionale, in virtù del quale numerosi Paesi non facenti parte dell'Unione Europea hanno provveduto ad adeguare spontaneamente le proprie legislazioni al fine di riavvicinarle a quella europea.

In quest'ottica, dunque, l'Unione Europea è riuscita gradualmente ad affermare, sulla scena internazionale, uno standard propriamente europeo in materia di tutela dei dati personali che ha conosciuto una rapida diffusione in tutto il mondo ed all'influenza del quale neppure il sistema giuridico degli USA è rimasto del tutto immune. Invero, nonostante i cedimenti di terreno in

occasione del confronto con gli Stati Uniti, altri paesi di grande tradizione giuridica come Canada, Israele e Giappone hanno ri-modellato la propria legislazione interna in materia di tutela di dati personali prendendo spunto proprio dal modello europeo.

La circolazione a livello internazionale di un modello europeo di tutela dei dati risulta particolarmente affascinante in quanto, se tradizionalmente è sempre stata l'egemonia economica e politica americana a determinare la diffusione ed il trapianto di schemi giuridici tipici di quel paese presso altri Stati oggi, quantomeno nel campo della tutela dei dati personali, si assiste ad un'interessante inversione di questa tendenza.

Allo stesso modo, non si possono neppure tacere gli sforzi innovativi compiuti dalla Commissione Europea in questo campo. Infatti, la Commissione Europea, invitata dal Parlamento a riflettere sulla condivisione dei dati personali con Paesi terzi aveva adottato, il 21 settembre 2010, un pacchetto di proposte riguardanti lo scambio dei dati PNR con stati terzi[585]. La comunicazione adottata dalla Commissione stabiliva dei principi cardine destinati ad essere contemplati da parte di qualsiasi accordo tra un Paese terzo e l'Unione Europea. Tra questi principi veniva previsto, anzitutto, che i dati raccolti avrebbero potuto essere utilizzati soltanto nel quadro della lotta contro il terrorismo e la grande criminalità e che solo le informazioni strettamente necessarie a questo fine sarebbero state oggetto di trasferimento.

Inoltre, veniva previsto che i passeggeri avrebbero avuto il diritto di consultare tali dati e di disporre di un diritto di ricorso amministrativo o giudiziario in caso di violazione della loro privacy, nonché l'istituzione di norme in materia di sorveglianza sulla corretta applicazione dell'accordo.

A seguito di tale comunicazione la Commissione ha presentato, il 2 febbraio 2011, una proposta di direttiva sui dati PNR tesa a sostituire la proposta di decisione quadro sull'utilizzo dei dati PNR presentata nel 2007[586] mentre, il 21 settembre 2012, è stata inoltrata una comunicazione relativa "*all'iniziativa globale in materia di trasferimento dei dati dei passeggeri aerei (PNR) i paesi terzi"*[587], vero e proprio "foglio di rotta" per la produzione normativa dell'Unione in tale materia e vertente su di un certo numero di criteri da rispettare tenuto conto, segnatamente, dei nuovi obblighi derivanti dalla Carta dei Diritti Fondamentali dell'Unione.

Infine, nel gennaio del 2012, la Commissione ha lanciato un ambizioso progetto di riforma dell'intero edificio normativo europeo in materia di tutela dei dati personali. Tale intervento legislativo che avrà luogo per mezzo di un regolamento e che coinvolge pure l'ambito della dimensione esterna, andrà a sostituire le legislazioni degli Stati membri in materia di tutela dei dati

[585] Propositions sur l'échange des données passagers Revue de droit des transports n° 11, Novembre 2010, alerte 109
[586] Proposition de directive relative aux données des passagers Revue de droit des transports n° 4, Novembre 2011, alerte 34
[587] COM(2010)492 final.

personali, comportando le modifiche e le innovazione che sono state descritte in un capitolo dedicato di questa tesi.

In conclusione, dunque, al termine di questo approfondimento nel campo della dimensione esterna della tutela dei dati personali nel diritto dell'Unione Europea, ci si sente di poter guardare al futuro con un certo ottimismo, potendo confidare nel fatto che la protezione di questo diritto fondamentale è oggi, assai più che in passato, saldamente ancorata al diritto primario dell'Unione, di cui costituisce elemento ispiratore nel campo della politica estera e della cooperazione internazionale con gli Stati terzi.

BIBLIOGRAFIA

- Marco Botta, Mario Viola De Azevedo Cunha "*La Protezione dei dati personali nelle relazioni tra USA e UE, le negoziazioni sul trasferimento dei PNR*", in Diritto dell'Informazione e dell'Informatica, 2010, 2, p. 315 (nota 1)
- Marsha Cope Huie; Stephen F. Laribee; Stephen D. Hogan, *The right to privacy in personal data: the EU prods the US and controversy continues*, in Tulsa Journal of Comparative and International Law, Spring 2002, Vol. 9 Issue 2, p391-469, 79p (nota 3)
- Matthew R. Van Wasshnova, "*Data protection conflicts between the United States and the European Union in the war on terror: lessons learned from the existing system of financial information exchange*", in Case Western Journal of International Law, 2007/2008, Vol. 39 Issue 1/2, p827-865, 39p (nota 4)
- Ugo Mattei, *Il Modello di Common Law*, Torino 2004 p. 250 (nota 5)
- Dorothee Heisenberg, "*Negotiating Privacy : the European Union, the United States, and personal data protection",* Londra 2005 (nota 6)
- Laura B. Pincus, Clayton Trotter, The disparity between public and private sector employee privacy protection: a call for legitimate privacy rights for private sector workers, in American Business Law Journal 1995 (nota 9)
- S. Warren e L. Brandeis, "*The right to privacy*", in *Harvard Law Review*, Boston 1890 (nota 13)
- William Prosser, *Privacy*, California Law Review Vol. 48 August 1960 No. 3 (nota 17)
- Shaman, Jeffrey M., *The right of privacy in state constitutional law*, Rutgers Law Journal, Summer 2006, Vol. 37 Issue 4, p971-1085, 115p (nota 23)
- Mason, *Judicial Activism: Old and New*, in 55 Va. Law Review 411 (1969)
- Malcolm, Joyce Lee Joyce Lee Malcolm, "Whatever the Judges Say It Is? The Founders and Judicial Review", The Journal of Law & Politics 26 no1 1-37 Fall 2010 (nota 36)
- Honorable Major B. Harding, Mark J. Criser e Michael R. Ufferman, "*Right to be let alone? Has the adoption of article I, section 23 in the Florida Constitution, which explicitly provides for a State right of privacy, resulted in greater privacy protection for Florida citizens?*" in Notre Dame Journal of Law, Ethic and Public Policy, 14 n. 2 945-1009 2000 (nota 41)
- Kathleen Anne Ward, *Williams vs. Attorney General of Alabama: does a constitutional right to sexual privacy exist?*, Thomas Jefferson Law Review Fall2008, Vol. 31 Issue 1, p1-24, 24p (nota 50)
- Antonio Gambaro, Rodolfo Sacco in "*Sistemi Giuridici Comparati*", Torino 2002, pp. 201 e ss (nota 61)
- Hong Haeji, "*Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao*", in Akron Law Review, 2005, Vol. 38 Issue 1, p71-111, 41p (nota 73)
- Frederick Z. Lodge, "*Damages under the Privacy Act of 1974: Compensation and deterrence*", in Fordham Law Review, March 1984, Vol. 52, p611-636, 26p (nota 74)
- Todd Robert Coles, "Does the Privacy Act of 1974 protect your right to privacy? An examination of the routine use exemption", in American University Law Review, Winter 1991, Vol. 40, p957-1002, 46p (nota 75)
- Amy S. Scarborough , "Nevada needs a Privacy Act: how nevadans are particularly at risk for identity theft", in Nevada Law Journal, Spring 2007, Vol. 7 Issue 2, p640-663, 24p (nota 78)
- Julianne M. Sullivan, "*Will the Privacy Act of 1974 still hold up in 2004? How advancing technology has created a need for a change in the system of record saving*", in California Western Law Review 39 no2 395-412 Spr 2003 (nota 79)

- Marco Pedrazzi, "*La Convenzione Europea sui diritti umani e il suo sistema di controllo", in "La tutela dei diritti umani. Norme, garanzie e prassi*", a cura di Laura Pineschi, Milano 2006 p. 236 (nota 81)
- Cesare Pitea, "L'interpretazione evolutiva del diritto al rispetto della vita privata e familiare in materia di libertà sessuale e di tutela dell'ambiente", in "La tutela dei diritti umani. Norme, garanzie e prassi", a cura di Laura Pineschi, Milano 2006 p. 428 (nota 86)
- Cfr. Chiara Bellini, "Privacy Informatica. Una Ricostruzione di ampio respiro", in "Diritto della Famiglia e delle Persone", anno 1999, fascicolo, 1 p. 459 (nota118)
- G. Cellamare, "*Tutela della vita privata e libera circolazione delle informazioni in una recente convenzione del Consiglio d'Europa*", in "*Rivista di Diritto Internazionale*", Anno 1982 Fascicolo 3 , pp 802 e ss. (nota 119)
- Claudia Faleri, "*Autonomia Individuale e diritto alla riservatezza*", in "*Rivista Italiana di Diritto del Lavoro*" anno 2000 fascicolo 3, p. 305 (nota 122)
- Lucia Serena Rossi, "*La protezione dei dati personali negli accordi di Schengen alla luce degli standards fissati dal Consiglio d'Europa e dalla Comunità Europea*", in B. Nascimbene (a cura di) "*Da Schengen a Maastricht:* ", Milano 1995, pp. 163 e ss. (nota 123)
- Luigi Ferrari Bravo, Enzo Moavero Milanesi, "*Lezioni di Diritto Comunitario*", Napoli 2002, p. 17 e ss. (nota 124)
- Giuseppe Tesauro, "*Diritto Comunitario*", Padova 2003, p. 130 e ss. (nota 128)
- Lucia Serena Rossi, "*Il parere 2/94 sull'adesione della Comunità Europea alla Convenzione Europea dei Diritti dell'Uomo"* in Diritto dell'Unione Europea, 1996 fasc. 3 p. 839 (nota 129)
- Maria Rosaria Donnarumma, "Il *processo di costituzionalizzazione dell'Unione Europea e la tensione dialettica tra la giurisprudenza della Corte di Giustizia e le giurisprudenze delle corti costituzionali*", in Riv. it. dir. pubbl. comunit. 2010, 02, 407 (nota 133)
- Chiti Edoardo, "*La tutela dei diritti dell'uomo nell'ordinamento comunitario*", in Giornale Dir. Amm., 1996, 10, 959 (nota 141)
- Girolamo Strozzi, "Diritto dell'Unione Europea, Parte Istituzionale", Terza Edizione Torino 2005 p. 250 (nota 142)
- R. Adam, A. Tizzano, "Lineamenti di Diritto dell'Unione Europea", Torino 2007, p. 122 e ss (nota 145)
- Pietro Manzini, *"Sull'irragionevole durata delle procedure comunitarie*", in Diritto dell'Unione Europea, 1999, 3 p. 511 (nota 151)
- Giulia Tiberi, "*Il diritto alla protezione dei dati personali nelle carte e nelle corti sovranazionali*", in Cassazione Penale, 2009, 11, p. 4667 e ss. (nota 167)
- Mario Cartabia, "*Principi inviolabili e integrazione europea*", Milano, 1995 pag. 134 e ss.. (nota 168)
- Denicolò-Palermo "*La riservatezza….senza riserve*", in *Diritto Pubblico Comparato ed europeo*, 2003, p. 1255 e ss. (nota 169)
- Fabienne Kauff-Gazin, "*Vers une conception de l'independence des autorités de régulation ? A propos de l'affaire C-518/07 Commission c. Allemagne* », in Europe n° 7, Juillet 2010, étude 9 (nota 191)
- Nicola Napoletano, "*La nozione di "campo di applicazione del diritto comunitario" nell'ambito delle competenze della Corte di Giustizia in tema di tutela dei diritti fondamentali*", in Diritto dell'Unione Europea, 2004, 4, p. 679 e ss (nota 197)
- Rocco Panetta, "*Trasferimento all'estero di dati personali e internet: storia breve di una difficile coabitazione*", in *Diritto dell'Unione Europea*, 2004, 4, pag. 1014 (nota 203)
- Alice Pisapia, "*Una sentenza additiva in punto di attuazione della direttiva sul ricongiungimento familiare",* in Giustizia Civile, 2007, 3, pag. 544 (nota 206)

- Fabio Macrì, "*La Corte di Giustizia sul diritto al ricongiungimento familiare: la sentenza Parlamento c. Consiglio*", in Diritto dell'Unione Europea, 2006,4, pag. 203 (nota 207)
- cfr. V.S. Negri, "La tutela dei diritti fondamentali nell'ordinamento comunitario alla luce del Trattato di Amsterdam", 1997 p. 788 e ss (nota 208)
- Federico Sorrentino "LA tutela multilivelli dei diritti", in Rivista Italiana di Diritto Pubblico Comunitario, 2005, 1 , pag. 91 e ss. (nota 211)
- Cristophe Caron, "*Appréciation de l'obbligation de communiquer des données à caractère personnel dans le cadre d'une procedure civile* », in « *La Semaine Juridique Entreprise et Affaires* » n° 9, 28 Février 2008, 1270 (nota 219)
- Alessandro Mantelero "*L'idra del peer to peer, tra tutela della privacy ed enforcement del diritto d'autore*," in Rivista Trimestrale di Diritto e Procedura Civile 2008, 4, 1482 e ss (nota 220)
- Gaia Mari, L'unione Europea impone di non sacrificare ad occhi chiusi la proprietà intellettuale sull'altare della privacy" in Diritto D'Autore, 2008,2, 289 e ss (nota 221)
- Pierluigi Di Maio, "Il rapporto tra diritto d'autore e diritto alla riservatezza. Recenti sviluppi nella giurisprudenza comunitaria", in Il Diritto D'Autore, 2010, 1, p. 20 (nota 222)
- Elsa Bernard, "Droits d'auteur et protection des droits fondamentaux", in Revue Europe n° 3, Mars 2008, comm. 98 (nota 223)
- Anna Saraceno "Note in tema di violazione del diritto d'autore tramite internet: la responsabilità degli Internet Service Providers", in Rivista di Diritto Industriale, 2011, 6, pg. 375 (nota 225)
- Laurence Idot, "Internet, piratage et obligations de filtrer les comunications éléctroniques » in Revue Europe n° 1, Janvier 2012, comm. 44 (nota 226)
- Ariane Siege, William Denny "*Survey of Privacy Law Developments in 2009: United States, Canada, and the European Union*", in The Business Lawyer 65 no1 285-307 N 2009 (nota 234)
- Luis Costa, Yves Poullet in "Privacy and the regulation of 2012", Computer Law & Security Review, June 2012, Vol. 28 Issue 3,p 9 p . 254262 (nota 236)
- Clark Boyd, "Global impact of Sony security breach" reperibile su http://www.theworld.org/2011/04/sony-security-breach/ aggiornato al 1 settembre 2012 (nota 238)
- Françoise Gilbert, "*EU Data Protection Overhaul, New Draft Regulation*" in The Computer & Internet Lawyer Vol 29 No 3 March 2012 (nota 244)
- Paul De Hert, Vagelis Papakonstantinou, "*The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals*" in Computer Law & Security Review 28 (2012) 130- 142 (nota 245)
- Gianantonio Benacchio "*Diritto Privato della Comunità Europea. Fonti, modelli, regole*", Cedam 2004 p. 178 (nota 254)
- Ioannis Ntouvas *"Single new law to reform data protection proposed by European Commission*" Journal of Computer, Media & Telecommunications Law; 2012 vol 17 issue 1, p. 3-4 (nota 273)
- Paolo Pallaro, "*Rapporti Commerciali tra UE e Stati Terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA*", in Diritto del Commercio internazionale 2000,03,753 (nota 281)
- Ryan Lowther, "*U.S. Privacy Regulations Dictated by EU Law: How the Healthcare Profession May be Regulated*" in Columbia Journal of Transnational Law 41 no2 435-54 2003 (nota 283)
- Lauso Zagato "*Il trasferimento di dati personali verso stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE*" in Dir. Comm. Internaz. 2008, 02, 297 (nota 285)

- C.-J. BENNETT, *Privacy Self-Regulation in a Global Economy: a Race to the Top, the Bottom or Somewhere else?* (Atti delle 22ª Conferenza internazionale sulla privacy e la protezione dei dati personali, Venezia, 28-30 settembre 2000). (nota 286)
- Santolli Justin "*The Terrorist Finance Tracking Program: Illuminating the shortcomings of the European Union's antiquated data protection directive"* in The Geo. Wash. Int'l L. Rev., 2008, 40,2, p. 563 e ss. (nota 287)
- Barbara Crulchfield George; Patricia Lynch, Susan J Marsnik "*US multinational employers: navigating through the "Safe Harbor Principles" to comply with the EU data privacy directive",* in American Business Law Journal 38 no 4 753-83 Summ. 2001 (nota 288)
- Giannaccari Andrea "Brevi note in tema di clausole contrattuali tipo per i trasferimenti di dati personali verso i paesi terzi" Danno e Resp. 2001, 10, 910 (nota 294)
- P. Pallaro, "*Libertà della persona e trattamento dei dati personali nell'Unione europea*", Milano, 2002, p. 47 (nota 303)
- Laura K. Donohue, "*Anti –Terrorist Finance in the United Kingdom and the United States*", 27 MICH J. INT'L L. 303,349 (2006) (nota 333)
- Jeff Gerth & Judith Miller, "*A Nation Challenged: Money Trail, US makes Inroads in isolating funds of terrorist groups"*, NY Times Nov. 5, 2001, at. A1 (nota 334)
- Adrienne Margolis "*Swift Response to preventing terrorist financing*", in Int Bar News 62 no. 1 F 2008 p. 12-15 (nota 336)
- Erich Lichtblau & James Risen, "*Bank Data Sifted in Secret. US Secretly tracks global bank data"*, L.A. Times, June 23, 2006 at A1.(nota 337)
- Fanchiotti Vittorio "*Voce "Processo Penale Statunitense (annali II-1 2008*)" in Enciclopedia del Diritto, Giuffré (nota 342)
- Katherine Scherb*, "Comment, Administrative Subpoenas for Private Financial Records:What Protection for privacy does the fourth amendment afford?",* WIS L. REV. 1075, 1075-85 (1996) (nota 343)
- Brand C. "*Belgian PM: Data Trasfer Broke Rules"* Associated Press. Reperibile su http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html. Consultato il 25.09.2012 (nota 349)
- Erich Lichtblau, Controls on bank-data spying impress civil liberties board" NY Times June 29, 2007 at A26 (nota 356)
- Patrick M. Connorton "Tracking terrorist financing through SWIFT: when U.S. subpoeans and foreign privacy law collide" Fordham Law Rev 76 n. 1 O 2007 (nota 358)
- Marc-Antoine Ledieu "CNIL – *Surveillance des transferts bancaires européens par les autorités américaines : vers une remise en cause des garanties négociées*" in Communication Commerce électronique n° 10, Octobre 2009, alerte 129 (nota 360)
- André PRÜM "*Bataille politique autour de SWIFT : la lutte contre le terrorisme doit compter avec le respect de la vie privée*", in Revue de Droit bancaire et financier n° 3, Mai 2010, alerte 9 (nota 373)
- Sylvia Kierkegaard "*US War on terror EU swift(ly) signs blank cheque on EU data*", in Computer Law & Security Law Review 27 (2011) 451 – 464 (nota 375)
- Rob Turner "*European Parliament Rejects SWIFT deal for sharing bank data with the US*" reperibile su http://www.dw.de/european-parliament-rejects-swift-deal-for-sharing-bank-data-with-us/a-5239595-1 aggiornato al 4.10.2012 (nota 384)
- Marie-Élisabeth MATHIEU "*Entrée en vigueur le 1er août 2010*" Revue de Droit bancaire et financier n° 5, Septembre 2010, comm. 183 (nota 395)
- E. Caprioli, " *Violation des règles propres aux données à caractère personnel et réseau SWIFT*", in Revue de Droit bancaire et financier n° 1, Janvier 2007, 34 (nota 401)
- Bruce Hoffmann, "*Inside Terrorism*", New York 1998, p. 67 (nota 403)

- Ioannis Ntouvas, "Air Passenger Data Transfer to the USA: the Decision of the ECJ and latest developments", in International Journal of Law & Information Technology, 16 n.1 73-95, 2008. (nota 406)
- D. Richard Rasmussen "Is international travel per se suspicion of terrorism? The dispute between the United States and European Union over passenger name record data transfers" , 26 Wisconsin International Law Journal, 551, 2008 (nota 407)
- Edward Hasbrouck *"What's in a Passenger Name Record (PNR)?",* consultabile su http://hasbrouck.org/articles/PNR.html aggiornato al 20.05.2010. (nota 408)
- James Fisher in *"What price does society have to pay for security? A look at the aviation watch list"* in 44 Willamette Law Review, 2008 (nota 411)
- Irfan Tukdi "*Transatlantic Turbulence: The Passenger Name Record Conflict"* in *"Thirty years of airline deregulation : a structure, conduct and performance review"* , 45 Houston Law Review 587, 2008 (nota 416)
- Christopher Patton, "*No man's land: the EU-US passenger name record agreement and what it means for the European Union's pillar structure*", in 40 George Washington International Law Review 527, 2008. (nota 424)
- Adam "*L'échange de données ò caractère personnel entre l'Union européenne et les Etats Unis. Entre souci de protection et volonté de coopération* » in Revue trimestrielle de droit européen, 2006 p.423 (nota 444)
- Alfredo Terrasi "*Trasmissione dei dati personali e tutela della Riservatezza:l'accordo tra Unione Europea e Stati Uniti del 2007*" in Rivista di Diritto Internazionale 2008, 2, p. 381 (nota 463)
- Pascal KAMINA Accord sur les données des passagers des compagnies aériennes Communication Commerce électronique n° 9, Septembre 2004, Alerte 181 (nota 468)
- Marc-Antoine LEDIEU « *L'adoption de la résolution sur les données des passagers et l'affaire SWIFT »* Communication Commerce électronique n° 4, Avril 2007, alerte 79 (nota 471)
- Flavien MARIATTE « *Rejet par la Cour des demandes de traitement accéléré des recours dans le dossier du transfert des données* PNR » in Revue Europe n° 12, Décembre 2004, comm. 400 (nota 447)
- Marc-Antoine LEDIEU « *Accord PNR - Pas d'urgence pour la CJCE »* Communication Commerce électronique n° 1, Janvier 2005, Alerte 22 (nota 478)
- Filippo Fontanelli, *La Corte di Giustizia e il "Favor Communitatis".Il percorso della giurisprudenza della Corte di Giustizia delle Comunità Europee sul fondamento normativo degli atti della Comunità e dell'Unione*" in Rivista Italiana di Diritto Pubblico Comunitario, 2010, 1 p. 183 e ss (nota 484)
- « *L'accord UE/USA sur le transfert des données passagers aux bons soins de la Cour »*, Révue Europe n° 10, Octobre 2004, Alerte 34 (nota 488)
- *Annulation d'un accord CE/USA sur le traitement et le transfert de données à caractère personnel par des transporteurs aériens* La Semaine Juridique Entreprise et Affaires n° 23, 8 Juin 2006, act. 264 (nota 493)
- Luigi Sbolci, "Conflitti tra Istituzioni dell'Unione Europea e Accordi Interistituzionali" Rivista di Diritto Internazionale, 2007,2, 9. 345 (nota 496)
- Lucia Serena Rossi "*Costituzionalizzazione" dell'UE e dei diritti fondamentali*", in "*Carta dei Diritti fondamentali e Costituzione dell'Unione Europea"* (a cura di Lucia Serena Rossi) Milano 2002, p. 263 e ss. (nota 497)
- M. Gisella Garbagnati Ketvel, *La giurisprudenza della Corte comunitaria in materia penale: verso un ravvicinamento tra i pilastri dell'Unione Europea*, in Diritto dell'Unione Europea, 2007, 2 p. 399 (nota 501)
- Flavien MARIATTE *La sécurité intérieure des États-Unis... ne relève pas des compétences externes des Communautés* in Révue Europe n° 7, Juillet 2006, étude 8 (nota 503)

- Valerie Michel « La *dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration* », note sous l'arrêt su 30 mai 2006, Parlement européen c. Conseil, aff. jtes C-317 et 318/04, Révue Trimestrielle Droit Européen, 3/2006, p.535 (nota 505)
- Flavien MARIATTE Transfert *des données PNR et protection des données personnelles* Europe n° 12, Décembre 2006, comm. 359 (nota 517)
- Loïc GRARD *Transfert de données personnelles des passagers* Revue de droit des transports n° 9, Octobre 2007, comm. 197 (nota 518)
- Flavien MARIATTE Conclusion du nouvel accord UE/USA sur le transfert des données PNR Europe n° 10, Octobre 2007, comm. 247 (nota 520)
- Loïc GRARD Nouvelle actualité des accords PNR . - Sûreté du transport aérien contre sécurité juridique Revue de droit des transports n° 3, Juillet 2012, repère 3 (nota 539)
- Sylvie PEYROU *Droits fondamentaux versus diplomatie, ou le pot de terre contre le pot de fer : réflexions sur la conclusion de l'accord PNR entre les États-Unis et l'Union européenne* » in Revue Europe n° 7, Juillet 2012, étude 8 (nota 541)
- Patrick E. Cole, "New challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws" in 17 N.Y.U J. INT'L L. & POL. 893, 897-98 (1995) (nota 522)
- Mike France, "*Once again, technology is outrunning privacy law*" in Business Week Online, Mar. 13 2000 at http://www.businessweek.com/technology/content/003/ep0313.htm aggiornato al 14.02.2013 (nota 554)
- David Aaron, "Privacy across the pond", Star Trib., June 4, 2000 at 11D.
- Kevin Bloss, "Raing or Razing the e-curtain" The EU directive on the protection of personal data", 9 Minn. J. Global Trade 645, 654 655 (2000) (nota 556)
- Wiliam J Long, Marc Pang Quek "Personal data privacy protection in an age of globalization: the UE-EU safe harbor compromise", in Journalof European Public Policy :3 June 2002 325-344 (nota 560)
- StephenJ. Kobrin "Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territoriale jurisdiction and global governance" in Review of International studies (2004), 30, 11-131 (nota 561)
- Juliana Gruenwald "Safe Harbor stormy waters", Interactive Week (30 ottobre 2000) disponibile su http://www.zdnet.com/zdnn (nota 569)
- Bell-Eder, Britney D.; Rynerson, Stephen D.; Soma, John T. "An analysis of the bilateral agreements between transnational trading groups: the US/EU E-commerce privacy Safe Harbor" in Texas International Law Journal 39 no 2 171-214 Wint 2004 (nota 570)
- John Graubert e Jill Coleman, "Consumer Protection and Antitrust Enforcement at the speed of light: the FTC meets the internet" in 25 Can-US L.J. 275-275 (1999) (nota 574)
- Julia Gladstone "The US Privacy balance and the European privacy directive: reflections on the United States Privacy Policy", Willamette J.Int'l L. & Dispute Res. 10, 10 (2000) (nota 575)
- Joel R. Reidenberg, E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717 (2001) (nota 576)
- Valentina Bazzocchi "*L'Accord entre l'Union européenne et les États Unis sur les données PNR*" consultabile su http://www.europeanrights.eu/index.php?funzione=A&op=5 (nota 579)