Università
Ca'Foscari
Venezia

Corso di Laurea magistrale (*ordinamento ex D.M. 270/2004*)
in Relazioni Internazionali Comparate

Tesi di Laurea

Ca' Foscari
Dorsoduro 3246
30123 Venezia

La protezione dei dati personali tra diritto UE e diritto internazionale

Relatore
Ch. Prof. Fabrizio Marrella

Laureando
Luca Righetto
Matricola 839695

Anno Accademico
2015 / 2016

INDICE

Capitolo 3 : La protezione dei dati personali e il “diritto all’ oblio”

Capitolo 4 : Il trasferimento di dati personali verso Paesi terzi: dal safe harbour all’ EU-US privacy shield

Capitolo 5 : La battaglia europea sui PNR e la sua evoluzione normativa

Capitolo 6 : SWIFT e le controversie del programma TFTP

Com’è definita l’identità?
In passato si diceva: “Io sono quello che dico di essere”.
Oggi, siamo quello che Google dice che siamo.
Siamo sempre meno persone, sempre più profili.
Stefano Rodotà

Abstract

The area of research of my thesis is the legislation on personal data protection.

Technology has advanced rapidly over the last few decades and now legislator must attempt with their work to keep up the ever increasing pace of change. With new technologies it is now incredibly easy to store enormous amount of informations and data. However, one of the main problems is that not always those data are kept at safe by the controller or processor.

A few years ago even a giant tech like Sony has been hacked and several personal data have been compromised. 77 million account were compromised and among the information contained there were also bank account and credit card card number. Sony waited one week to let their consumers know of the breach. Such a long wait expands the damage caused to consumers by the breach. Within the EU legal framework Sony should have notified immediately what had happened to a supervisory authority. Also, in the EU legal framework, controllers of personal data have to provide a very high level of protection for collected data.

Moreover, the path choose by European legislator includes privacy by design: in a digital world where privacy is jeopardised by new technologies the remedy should originate from technologies themselves.

Privacy should be a requirement in IT system. It is not something that should be think about at last, but since the beginning of the development of each software. For example, the architecture of a healthcare records should be built by having in mind the privacy concerns of patients. Or, more in general,

the collection of data should be limited to those strictly necessary and should always need a consent from the subject, the use of data should be limited to its initial purpose, and there should be reasonable security safeguards and openness to individual.

No other country has a high level of protection of personal data that could be compared to the European level. However, in a globalised world where huge amount of informations can move instantly from one side of the world to the other, it is particularly important to have a worldwide shared legislation about personal data protection: for example, everywhere a high level of protection must be required when personal data are stored.

Most of the focus of my thesis will be on European legislation because Europe has been the major promoter of personal data protection for a long time. Others, like the US, have chosen to follow a path that gives priority to security over privacy.

There is one key different between European history and American history that can explain why we have choosen divergent road over years: it is the experience of life under a totalitarian regim.

During the first half of the XX century European country had to struggle against totalitarianism. As Benito Mussolini said, this political system wants “everything within the state, nothing outside the state, nothing against the state”. A totalitarian regim wants a complete control over individuals and society and this means no privacy, no own ideas outside the propaganda of the regime, and no choice.

And privacy is essential for human being, because without it individuals cannot freely express themselves. Therefore, privacy is not just a fundamental liberty but it is also an essential basis for other fundamental rights.

Without any doubt privacy is a fundamental liberty of individuals but its protection might prejudice security interests or obstruct other liberties.

For example, there is a possible conflict between privacy and freedom of expression. In many sentences of the European Court of Justice and of the the European Court of Human Rights, Courts had to find the right balance between those two rights. Usually, an important element to tip the balance is whether the subject is a public figure or not. Also, to move the needle they have to consider if the matter is of public interest. Regarding this point, there always have to be also proportionality between the burden that some informations can cause to a person and the public interest that they may contain.

Correlated to the freedom of expression there is another modern hurdle for privacy: the digital world, especially social network.
Mark Zuckemberg said that “privacy is no longer a social norm”, however this is a dangerous statement for individuals. Human beings have not a perfect memory: after a few years memories fade away and we start forgetting events of the past. Instead, the digital world has a perfect memory, a place where nothing is erased. All contents that are loaded on the web stay there, never forgotten. This can create enormous problems. Some facts related to an episode of the past can be brought out anytime like they were actuality. A single error happened twenty years before and completely forgotten by a human mind, can come up as a ghost from the past on the internet.
There should be a balance between what really matters and could be of public interest and what instead should be forgotten and be left in the darkness created by time. Some facts of the past could damage an individual without any proportionality.

It’s not only the freedom of expression but also the need of security that is used to justify restrictions and interferences on the citizens’ liberties.

The balance between privacy and security can be seen from an economic perspective as a trade-off between one another. Choosing to improve security often means to reduce privacy.
However, it would be important to consider security as an exception that should be invoked only on strict conditions: the priority should be to protect our privacy and other liberties.

Another big problem that is becoming each day of a greater concern is terrorism. The menace of terrorism has brought a sentiment of dread in the heart of people and many politicians have used this fear to adopt extreme mesures that could possibly increase security but without any doubt reduce privacy. Not always these mesures are really necessary. There is always a choice to use some more privacy-friendly instruments.
On 2013, the revelations made by Edward Snowden, a former National Security Agency subcontractor, had showed to the world's eyes that a line was been crossed by American security agencies.
There are no reasons, terrorism included, that can justify a mass-surveillance like the one operated by the NSA. The clandestine surveillance program has involved massive amounts of intercepted data, and bugging UN officies, embassies and also political leader like Angela Merkel.
Fighting terrorism means also to fight for some important values and putting in act mesures that obliterate individual's liberties means having already lost this war. In a democracy the most important things should be to protect the fundamental rights of individuals.

This thesis aims to analyse what have been the greatest improvements over the last few years on the field of personal data protection, and also to point out some controversy on this theme.

On the first chapter I will offer an outlook of how the concept of privacy has evolved throughout the year, and how at a certain point this has included also the protection of personal data.

On the second chapter I will describe the main regulations that protects privacy in Europe. The first important international treaty is the Convention for the Protection of Human Rights and Fundamental Freedoms, that entered into force on 3 September 1953. The Convention also established the European Court of Human Rights: this Court is an essential instrument to protect individuals who feels their rights have been violated under the Convention. In particular the article 8 of the Convention protect the right to respect for private and family life: “everyone has the right to respect for his private and family life, his home and his correspondence” and “there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”. An article that through the sentences of the European Court of Human Rights has been given a broad interpretation. Not only it avoids a State to interfere with rights of the indiviuals but sometimes it provides also positive obligations: an obligation for the State to grant the effective enjoyment of this right.

Instead, the European Union adopted in 1995 a Data Protection Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This has been a first attempt to armonyse each European data protection laws and also to adopt high standards for such protection.

But with time many things have changed and this law was no more enough since it has to deal with technologies that wasn't even possible to think about when it was first written more than twenty years ago.

Therefore, on 2016 a new regulation has been adopted and will enter into application on 25 May 2018. The Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC(RGPD) will strengthen and unify the European data protection.

On the third chapter, I will analyse the so called "right to be forgotten". In May 2014, the European Court of Justice, on the case Google Spain v AEPD and Mario Costeja González, ruled that Google had an obligation to delete link to incorrect or outdated informations. Now, this right is protected by the Article 17 of the RGPD: "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" if it meets certain condition written in the Article.

But there is still much controversy around this right that is protected in Europe but is seen like an interference on freedom of expression somewhere else.

On the forth chapter, I will focus on the transfer of personal data from a European State to third countries. Article 25 of Directive 95/46/EC says that "member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection".

Until now the Commission has recognized only Andorra, Argentina, Canada, Faeroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland and Uruguay as States that provide adequate protection.

United States and European Union had found a mechanism called “Safe Harbour” to transfer personal data from the EU to the United States and at the same time to comply with EU data protection requirements. However, this mechanism has been declared no longer valid from the European Court of Justice. A new mechanism called “Pricacy Shield” has replaced the “Safe Harbour” and now is the framework for the exchanges of personal data for commercial purposes between the EU and the United States.

On the fifth chapter, I will go through the battle between the European Parliament and the European Commission on the ground of Passenger Name Record. A passenger name record (PNR) is a record collected in a database of a computer reservation system (CRS) that store many information about passengers travelling on an airline such as name, address, ticketing details, itinerary and much more. Since 9/11 the United States has decided to use PNR has a tool to fight terrorism, by matching data conteined on the PNR with criminal databases.

However, the amount of information contained in a PNR is huge and some of these informations have a sensitive nature.

On the sixth chapter, I will analyse the development of the terrorist finance tracking program. After the 9/11 the U.S. Government understood the importance to track terrorist money flows in order to uncover terrorist cells and find their networks.

With this goal in mind the U.S. Treasury Department required the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to transmit them financial transaction informations. SWIFT is a Belgium company that

had his server also in America and it stored there the information of most of the world finance transactions.

When SWIFT moved its American server in the European Union, the U.S. Government had to negotiate an agreement with the EU.
In this case, the amount of data transfer is huge, therefore it hasn't been an easy process the one to find the right balance and sign an agreement.

The legal framework of protection of personal data is changing fast. Currently the EU has the most advanced law that regulates protection of personal data. EU should take the role of the leader and show to the rest of the world his way.

Introduzione

Perché la protezione dei dati personali è importante?

Quello dei dati personali è un tema che negli ultimi anni ha guadagnato una sempre maggior rilevanza, soprattutto per via dei rapidi progressi ottenuti nel campo informatico. Da una parte, ci sono stati nel giro di soli due decenni quei progressi che hanno ampliato notevolmente la capacità di conservare dati e informazioni: la mia generazione è cresciuta vivendo il rapido passaggio dai floppy disc che potevano contenere poche megabyte di informazione agli anni dei CD che permettevano di contenere gigabyte di dati fino ad arrivare ai giorni odierni dove i server messi a disposizione dai servizi cloud riescono a immagazzinare terabyte e petabyte di dati. Dall'altra parte, di pari passo ai progressi nel campo della conservazione dei dati, vi sono stati la diffusione e lo sviluppo di internet. Oggigiorno non è più necessario archiviare in voluminosi scaffali migliaia di pezzi di carte: tutto viene caricato e salvato nel web e risulta facilmente accessibile da ovunque e velocemente scambiabile senza limitazioni geografiche. Infine, gli anni più recenti hanno visto l'esplosione del fenomeno dei social network, le piattaforme che per eccellenza vedono caricati giornalmente in essi una gran mole di dati personale e che per certi versi hanno fatto confondere se non perdere i tradizionali confini della privacy. Le enormi quantità di dati personali che girano nella rete sono al sicuro? Non molto. I social network e i motori di ricerca ricavano gran parte dei loro guadagni proprio grazie alla vendita dei dati personali dei loro utenti. In quanto alle aziende che hanno a che fare in

via informatica con la gestione di dati personali conservati in server, esse spesso non garantiscono dei livelli di protezione dei dati raccolti adeguati, dimostrandosi in più di un'occasione non sono all'altezza del ruolo di responsabile di quei dati: annualmente sono moltissime le brecce in sistemi informatici aziendali che rivelano i dati inseriti dai loro utenti. Persino un colosso nel campo della tecnologia come Sony si è rivelato un custode inaffidabile quando nel 2011 degli hacker hanno fatto breccia nei server della multinazionale giapponese trafugando i dati personali di quasi 77 milioni di persone, tra cui nome, indirizzo, mail e in alcuni casi le informazioni sulle carte di credito. Inoltre in quel caso Sony attese 7 giorni prima di avertire gli interessati[1]. Un' enormità considerato che in ballo c'erano anche dati quali i numeri delle carte di credito. Se a livello globale fosse applicata la normativa sulla protezione dei dati, la società nipponica sarebbe stata sanzionata per non aver avvertito gli interessati in modo tempestivo. Ma al momento così non è. Anzi, pochi sono i paesi che prevedono un adeguato livelllo di tutela dei dati personali.

È chiara dunque l'importanza di raggiungere una normativa condivisa che metta nelle condizioni di garantire la sicurezza dei dati personali delle persone richiedendo elevati livelli di protezione da parte di coloro che gestiscono questi dati personali. Nonché vi sia la presenza di protocolli che permettano di informare tempestivamente le persone nel malaugurato caso in cui avvenga una breccia nei sistemi, in modo che gli utenti colpiti possano correre ai ripari.

Infine, negli ultimi anni c'è stato ulteriore fattore che ha influenzato pesantemente questa materia: il terrorismo. In seguito agli attentati del 11 settembre 2001 negli Stati Uniti la strada percorsa è stata quella di un

[1] Keith Stuart and Charles Arthur, 27 aprile 2011, *PlayStation Network hack: why it took Sony seven days to tell the world*, The Guardian, Consultabile su: https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony Accesso 2 settembre 2016

maggior controllo a scapito della privacy e della protezione dei dati personali. Diversamente, l'Unione europea (UE) ha prediletto la salvaguardia della protezione dei dati personali. Tuttavia, i recenti attentati che hanno colpito Parigi e Bruxelles nel 2016 potrebbero avere ripercussioni nel modo in cui finora i legislatori europei si sono approcciati alla materia. Sicuramente gli attentati hanno pesato non poco nella scelta del Parlamento europeo di approvare una direttiva europea sui *Passenger Name Record* (PNR).

Allo stato attuale non esiste una legislazione sulla protezione dei dati personali che sia condivisa a livello internazionale. Parte delle difficoltà nel raggiungere qualsiasi accordo insorgono per via del fatto che si tratta di un campo moralmente controverso in cui si sono visti e si vedono tuttora fronteggiare il diritto d'espressione contro il diritto alla privacy, oppure la sicurezza nazionale contrapposta ancora una volta alla privacy. Finora l'Europa si è elevata a paladina della difesa dei dati personali e recentemente l'UE ha approvato un regolamento che finalmente uniformerà la normativa sulla protezione dei dati personali fra i suoi stati membri. L'UE è l'unica organizzazione internazionale che al momento potrebbe essere in grado di far partire un processo che possa portare alla formazione di accordi internazionali che salvaguardino la protezione dei dati personali.

Questa tesi andrà ad analizzare la recente evoluzione del diritto nel tema della protezione dei dati personali all'interno del panorama europeo e nei suoi rapporti con le realtà più importanti che lo circondano, mostrando luci ed ombre della strada finora intrapresa dai legislatori e valutando anche i contrasti con le altre realtà mondiali in particolare statunitense.

Il primo capitolo sarà dedicato ad un'analisi per lo più filosofica dell'evoluzione dei concetti di privacy e di protezione dei dati personali.

Il secondo capitolo analizzerà i principali strumenti legislativi che sono stati adottati negli anni nell'ambito della protezione della privacy e dei dati personali.

Il terzo capitolo è dedicato al cosiddetto “diritto all’oblio”, una novità degli ultimi anni che è nata al centro di mille controversie.

Il quarto capitolo sarà dedicato allo studio del trasferimento dei dati personali verso paesi terzi ed in particolar modo alle controversie che si sono originate in tal senso verso con gli Stati Uniti.

Il quinto capitolo si focalizzerà sullo strumento degli accordi PNR, volti a condividere informazioni sui passeggeri dei voli al fine di combattere il terrorismo.

Il sesto capito sarà incentrato sulla vicenda che ha coinvolto la società belga SWIFT e sugli accordi legati al programma statunitense *Terrorist Finance Tracking Program* (TFTP).

Capitolo 1
I concetti di privacy e protezione dei dati personali

1.1 La nascita del concetto di privacy

Se cerchiamo nel Devoto-Oli la definizione di privacy, potremo osservare che questo termine viene espresso nel seguente modo: “l'ambito gelosamente circoscritto della vita personale e privata”[2]. Quello della privacy è un concetto estremamente moderno, che risale a non più di 150 anni circa, ma è allo stesso tempo un aspetto da sempre inerente la natura umana. La privacy è il motivo per cui da millenni l’uomo ha costruito dei muri per limitare la sua proprietà privata: nella natura umana vi è un bisogno intrinseco di differenziare una sfera individuale privata, in cui si può agire senza temere gli sguardi e i giudizi altrui, ed una sfera individuale pubblica, nella quale ad ogni propria azione verrà dato un peso da parte della società.

Con la nascita delle società, guardando ad esempio al tempo della *polis* greca, cominciamo a trovare la distinzione fra una sfera di vita privata e una pubblica. Tuttavia, nell’antica Grecia la visione era molto diversa da quella odierna: a quel tempo l’accento era posto sulla privazione che una vita trascorsa nella sfera domestica comportava. Aristotele aveva definito l’uomo come un “animale sociale-politico”[3], e per questo motivo una persona che viveva nel privato era considerata come se non esistesse, e d’altronde era a quel tempo la descrizione della condizione degli schiavi. Un altro grande

[2] Dizionario Devoto-Oli Digitale 2016
[3] Concetto di *“politikòn zôon”* di Aristotele espresso nel trattato Politica

filosofo di quel tempo, Platone, avrebbe voluto che l'ambito pubblico avvolgesse anche la vita individuale delle persone[4]. Ciononostante un aspetto di privacy non era esente nemmeno nella cultura ellenica: il padre degli dei, Zeus, veniva venerato in ambiente domestico, spesso nel cortile antistante l'abitazione, come Zeus Herkeios, nelle vesti di protettore del recinto della casa e difensore dello spazio privato dall'esterno[5].

Già qualche secolo più tardi, nell'antica Roma veniva data assoluta importanza alla sacralità del focolare domestico, in base alla quale era vietato invadere la vita privata dei cittadini romani[6].

Sarà successivamente con l'avvento del Cristianesimo che la dimensione privata dell'individuo comincerà ad assumere caratteristiche più moderne. Con la diffusione della moralità cristiana, viene data una grossa importanza al rispetto degli altri, il che implica di evitare di importunare le altre persone e non ficcare il naso nella vita altrui, sulla quale alla fine scenderà il giudizio divino.

Si apre anche un filone filosofico nuovo. Ad esempio, per Locke i beni privati sono più necessari e urgenti delle cose del mondo comune[7].

Avvicinandosi poi sempre più al periodo moderno vi è anche la conquista del valore dell'intimità, che è stata descritta come "un'evasione dal mondo esterno nel suo insieme per rifugiarsi nell'interiore soggettività individuale, che era stata riparata e protetta in precedenza dalla sfera privata"[8]. È in quel contesto che Jean-Jacques Rousseau si ribellerà contro la corruzione del cuore umano provocata da parte della società. L'intimità non ha un posto tangibile né nel mondo, né nella società, ma ha ragione di esistere esclusivamente nella sfera del privato[9]. L'uomo ha bisogno dunque di uno

[4] Concetti espressi da Platone nel trattato La Repubblica(*Politéia*)
[5] Jon D. Mikalson, 2009, *Ancient Greek Religion,* Wiley-Blackwell
[6] Hannah Arendt, 1958, *Vita activa: la condizione umana*, Bompiani
[7] vedi *Il secondo trattato sul governo* di Locke e il rapporto tra proprietà privata e la "cosa comune"
[8] Arendt, nota 6
[9] Arendt, nota 6

spazio anche per la sua interiorità. Ci deve essere un bilanciamento tra la vita nella società e un ambiente riservato.

Ma se da una parte l'uomo comincia ad apprezzare il valore dell'intimità, dall'altra la tecnologia ha provveduto anch'essa a mutare la quotidianità delle persone con numerose scoperte: in particolare, a cambiare radicalmente la vita sociale delle comunità sono la stampa e l'editoria.

È proprio per difendere le persone dalla possibile invasione nelle loro vite da parte della stampa che troviamo il primo caso di una legislazione che tra i suoi articoli provvede anche alla protezione della privacy, pur senza riferirsi ad essa con quel termine, che ha un'origine più recente. L'11 maggio 1868 in Francia viene emessa la *Loi relative à la presse* (legge sulla stampa). In essa viene proibita la pubblicazione di fatti relativi alla vita privata degli individui a meno che i fatti non fossero già pubblici o pubblicati con il consenso dell'individuo[10].

La nascita concettuale del diritto alla privacy viene solitamente attribuita a due giovani avvocati, Samuel D. Warren e Louis D. Brandeis[11]. I due vivevano a Boston in un'epoca in cui la carta stampata si stava evolvendo, con il passaggio al fotogiornalismo, e con la pubblicazione di eventi mondani e pettegolezzi. Vivendo in quel particolare momento storico, i due furono ispirati a pubblicare nel dicembre 1890 un saggio intitolato '*The right to privacy*'. Warren e Brandeis definirono la privacy come un'estensione del diritto di proprietà che andava ad includere aspetti non materiali come i sentimenti, i pensieri e le emozioni, che fino a quel momento non avevano ancora ricevuto alcuna tutela. Lo definirono come un diritto negativo, nello specifico usarono l'espressione "*right to be let alone*", cioè un diritto a essere lasciati soli[12]. Inoltre Warren e Brandeis invitano i giudici americani a

[10] Gloria González Fuster, 2014, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer
[11] idem
[12] Dorothy J. Glancy, 1979, *The invention of the right to privacy*, Arizona Law Review

cominciare a garantire il diritto alla privacy nelle loro sentenze, e a farlo diventare un diritto di *Common Law*. Tuttavia i tempi non erano ancora maturi e la voce dei due avvocati rimase per lo più inascoltata.

È sempre quando rischiamo di perdere qualcosa che davamo per scontato che ci accorgiamo della sua importanza. Un appello alla privacy giunse nel 1955 da William Faulkner, scrittore Premio Nobel nel 1949, che aveva vissuto sulla propria pelle l'invasione della sua privacy da parte dei giornalisti dopo aver ricevuto ad Oslo l'onorificenza per le sue opere letterarie. Faulkner scrive un breve trattato nel quale esprime la sua disillusione per il Sogno Americano, venuto meno in quanto nella terra della libertà e della democrazia la gente non riesce più a percepire dove stia il giusto confine tra ciò che deve essere privato e ciò che può essere reso pubblico. Per Faulkner il vero colpevole è il pubblico: curioso e mai sazio di invadere la vita privata altrui. La stampa deve vendere e perciò si adegua a queste richieste in un gioco al ribasso che porta ad una continua erosione della vita privata degli individui. Infine ribadisce l'importanza della privacy "*quella privacy che, sola, consente all'artista, allo scienziato e all'umanista di funzionare. O per salvare la vita stessa*"[13]. Quest'ultimo aspetto è condiviso anche dalla Arendt che esprime la necessità "*dell'esser soli con l'idea, l'immagine mentale della cosa da creare*"[14]. Per lei la privacy, ovvero la garanzia dell'isolamento, è la condizione necessaria senza la quale nessuna opera può essere prodotta[15].

Un ulteriore contributo a teorizzare la privacy è fornito dal giurista William Prosser nel suo articolo "*Privacy*", pubblicato nel 1960. Prosser divideva la violazione del diritto alla privacy in quattro categorie: la prima è un'intrusione in uno spazio privato, la seconda è la rivelazione pubblica di fatti privati personali, la terza è mettere qualcuno in cattiva luce in modo pubblico, e la

[13] William Faulkner, 1955, *Privacy*, Piccola Biblioteca Adelphi
[14] Arendt, nota 6
[15] idem

quarta ed ultima categoria è l'utilizzo per il proprio guadagno del nome altrui o di altri suoi dati personali, senza averne il consenso[16].

Il diritto che si è dunque configurato con il saggio di Warren e Brandeis prima e con il lavoro di Prosser in seguito è un diritto negativo in cui la privacy mira a proteggere da un torto.

Nel frattempo in Europa la terribile esperienza dei regimi totalitari è servita da lezione al Vecchio Continente per comprendere l'importanza della privacy.

Uno dei principali elementi comuni ai vari totalitarismi è il fatto che essi miravano all'alienazione dell'individuo, privandolo della libertà e facendogli abbracciare l'ideologia del partito, togliendogli la facoltà di scelta, ma confortandolo con la propaganda in una rassicurante dittatura [17]. L'uomo veniva trascinato in un mondo fittizio in cui non pensava, nel quale invece doveva limitarsi a seguire le regole. I regimi totalitari volevano quindi esercitare un controllo totale sull'individuo, che andava dunque a scapito della sua sfera privata per assicurarsi la sua fedeltà totale. Il partito si inserisce nella vita privata delle persone ed agisce non diversamente dal Grande Fratello di George Orwell, che controlla giorno e notte la vita dei cittadini per assicurarsi che questi siano fedeli alla volontà del capo[18].

Se un uomo viene privato della sua vita privata, anche le sue capacità di agire e pensare vengono limitate e la perdita di libertà si espande ad ogni altro aspetto della sua vita, rendendolo più un automa che una persona.

L'idea dell' "*uomo di vetro*" che non ha nulla da nascondere è una metafora totalitaria basata sulle mire dello Stato a conoscere anche gli aspetti più intimi della vita dei propri cittadini[19]. La privacy, per converso, diventa dunque un

[16] Neil M. Richards e Daniel J. Solove, 2010, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887

[17] Hannah Arendt, 1948, *Le origini del totalitarismo*, Piccola biblioteca Einaudi

[18] George Orwell, 1949, *1984*, Mondadori

[19] Stefano Rodotà, 23 ottobre 2011, *L'ansia di sicurezza che cancella i diritti*, articolo su La Repubblica, Consultabile su:

prerequisito della democrazia[20].

1.2 Privacy e protezione dei dati personali

Come abbiamo visto lo sviluppo del concetto di privacy è molto recente e la nascita di un diritto che la tutela arriva solamente nel secolo scorso. Quello della protezione dei dati personali è un tema ancor più moderno di quello della privacy.

La tutela dei dati personali è un diritto la cui importanza si è accresciuta a mano a mano che i mezzi tecnologici hanno consentito alle informazioni di girare per il mondo in modo sempre più rapido e vorticoso. In una realtà dove i dati personali si muovono incessantemente, la privacy è diventata così anche il diritto di una persona ad avere il controllo sulle informazioni che la riguardano.

Nel 1997, ad esempio, Roger Clarke suddivideva la privacy in quattro categorie: (1) la privacy dell'individuo(inteso in termini fisici), (2) la privacy dei comportamenti umani, (3) la privacy delle comunicazioni personali e (4) la privacy dei dati personali[21].

Altri giuristi hanno ripreso il modello di Clarke e lo hanno allargato suddividendo la privacy in sette tipi: (1) la privacy delle persone, (2) la privacy dei pensieri e dei sentimenti, (3) la privacy dell'ubicazione e dello spazio, (4) la privacy dei dati e immagini personali, (5) la privacy del comportamento e delle azioni, (6) la privacy delle comunicazioni e (7) la privacy di

---

http://www.repubblica.it/online/speciale/ventitreottobredue/ventitreottobredue/ventitreottobredue.html Accesso 16 Settembre 2016

[20] Hosein, Rouvroy, Poullet, 2009, *Reinventing Data Protection?*, Springer

[21] Roger Clarke, 1997, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, Xamax Consultancy, Consultabile su: http://www.rogerclarke.com/DV/Intro.html

associazione[22].

Possiamo così notare che il diritto alla protezione dei dati personali è stato a lungo incorporato all'interno del diritto alla privacy, e solamente negli ultimi decenni si è giunti al punto in cui questi due diritti sono cominciati a essere anche (ma non sempre) considerati in modo distinto.
Come vedremo più dettagliatamente nel capitolo seguente, è stato con la proclamazione della Carta dei diritti fondamentali dell'UE[23] che per la prima volta si è voluto elevare la protezione dei dati personali a diritto fondamentale, tanto quanto lo sono il diritto alla privacy o il diritto di espressione.
Rodotà ha definito la Carta dei diritti fondamentali dell'UE come il punto finale di un'evoluzione che ha portato ad una separazione della privacy e della protezione dei dati personali[24].
Proteggere i dati personali di una persona significa dunque da una parte tutelare la sua privacy, ma dall'altra asserve anche ad altri obbiettivi, ed è per questo che con il tempo è stato riconosciuto come un diritto a sé stante. In primis, per molti giuristi, tra i quali Rodotà, Rouvroy e Poullet, la legislazione sulla protezione dei dati personali si basa su importanti valori etici, uno su tutti quello la garanzia della dignità umana[25].
L'enorme raccolta di dati, tra cui anche quelli sensibili, potrebbe in taluni casi favorire situazioni di discriminazione, e dunque un diritto alla protezione dei dati diventa essenziale per garantire l'eguaglianza. Nel caso di dati sanitari diventa parte necessaria per garantire il diritto alla salute. Così come la tutela dei dati sulle opinioni devono salvaguardare le libertà di associazione, espressione e culto. La protezione dei dati personali diventa quindi una

[22] Finn, Wright, and Friedewald, 2013, *Seven types of privacy* in S. Guthwirth e altri, European Data Protection: Coming of Age, Springer
[23] v. capitolo 2.1
[24] Stefano Rodotà, 2009, *Data Protection as a Fundamental Right* in S. Guthwirth e altri, Reinventing Data Protection?, Springer
[25] Rodotà, Rouvroy, Poullet, 2009, *Reinventing Data Protection?,* Springer

componente essenziale di una pluralità di libertà dell'individuo[26].

Secondo i giuristi De Hert e Gutwirth la privacy e la protezione personale sono due facce della stessa medaglia, due diritti differenti eppure complementari. Tuttavia, per funzionare in modo efficace questi due ambiti devono restare distinti. De Hert e Gutwirth facendo un confronto evidenziano che il diritto alla privacy è, in termini generali, un diritto sostanzialmente negativo, di non interferenza, che protegge la zona d'ombra (ciò che è privato) dell'individuo; all'opposto, il diritto alla protezione dei dati personali si esprime come una richiesta di trasparenza da parte dei detentori di dati personali. Secondo De Hert e Gutwirth la privacy crea uno scudo attorno alle persone garantendo loro una zona di autonomia e libertà in cui queste si possono muovere, mentre nella protezione dei dati personali il focus è sulla trasparenza dei detentore dei dati personali e sul consegnare un potere di controllo nelle mani delle persone[27].

Il diritto alla protezione dei dati è nato con due caratteristiche peculiari che lo contraddistinguono: il consenso e la proporzionalità. In altre parole, per poter raccogliere dei dati personali deve sempre essere richiesto il consenso dell'individuo, e l'uso di quei dati essere proporzionale allo scopo, cioè i dati che vengono manipolati possono essere usati esclusivamente ai fini per cui sono stati inizialmente raccolti.

Alcuni giuristi vedono però dei limiti in questi due punti essenziali. Ad esempio, Bygrave e Schartum mettono in risalto il fatto che il consenso sia spesso un atto formale, raramente libero e in molti casi inevitabile; mentre, per quanto riguarda la proporzionalità, essa non è talvolta un criterio sufficientemente limitante. La loro proposta alternativa consiste in un esercizio collettivo del consenso che, per quanto difficile da realizzare,

[26] Stefano Rodotà, 16 settembre 2004, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati: *Privacy, libertà e dignità*

[27] De Hert e Gutwirth, 2009, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation* in S. Guthwirth e altri, Action in Reinventing Data Protection?, Springer

consentirebbe di rafforzare la posizione dell'individuo nei confronti dei detentori di dati[28].

A questo proposito Berkvens propone come modello l'approccio alla privacy dei consumatori adottato da alcune leggi statunitensi. Un approccio collettivo renderebbe possibili class action che potrebbero rafforzare il potere effettivo della protezione dei dati personali[29].

1.3 Il "costo opportunità" della privacy e protezione dei dati personali rispetto a sicurezza e libertà di espressione

Il fatto che la protezione dei dati personali tuteli la privacy delle persone, e così facendo salvaguardi una pluralità di libertà dell'individuo, non è in contraddizione con la possibilità che al tempo stesso si vadano a ridurre altre libertà fondamentali.

Vi sono numerosi autori che analizzano la privacy con un modello di "costo opportunità", dove la sua tutela viene contrapposta ad altri diritti, in particole la sicurezza nazionale e la libertà di espressione. Da un certo punto di vista questo *trade-off* rappresenta un aspetto della quotidianità delle persone, basti pensare che nel momento in cui un individuo autorizza al trattamento dei suoi dati personali ha già acconsentito ad una riduzione della sua privacy in cambio dei servizi ottenuti[30].

---

[28] Lee A. Bygrave and Dag Wiese Schartum, 2009, *Consent, Proportionality and Collective Power* in Reinventing Data Protection?, Springer

[29] Jan Berkvens, 2009, *Role of Trade Associations: Data Protection as a Negotiable Issue* in S. Guthwirth, Reinventing Data Protection?, Springer

[30] Per maggiori approfonfimenti sulla concezione di privacy come "costo-opportunità" rispetto ad altre libertà rimando a Serge Gutwirth, 23 marzo 2011, *Privacy and emerging fields of science and*

Uno dei rapporti più discussi e controversi è quello tra la privacy e la sicurezza nazionale. Solitamente a livello europeo la visione preferita è quella di mantenere la priorità per le libertà dei cittadini, considerando la sicurezza come una sorta di eccezione che può essere invocata solamente sotto rigide condizioni. Alcuni giuristi, come Alonso-Blas, sono invece meno favorevoli a questo approccio. Lei ritiene che il lavoro della polizia debba essere tenuto in considerazione diversamente e ad esso debbano essere fornite regole fatte su misura applicabili al campo della sicurezza pubblica[31].

Negli ultimi anni la minaccia del terrorismo ha portato, specialmente in America, a preferire più spesso nel computo del "costo opportunità" la sicurezza alla privacy.

A tal riguardo, la Chandler nota però che troppo spesso la privacy viene sacrificata prematuramente in nome della sicurezza nazionale. Per lei, prima di prendere qualsiasi decisione in merito, la valutazione dovrebbe essere fatta valutando in modo preliminare alcune questioni: (1) se le misure di sicurezza contemplate offrono davvero alcuna sicurezza; (2) se ci sono metodi alternativi, meno invasivi per la privacy, che raggiungano gli stessi risultati di sicurezza; (3) se il costo della sicurezza vale il costo totale delle misure di sicurezza adottate; (4) se il sacrificio è distribuito in modo giusto, in modo che la maggiore sicurezza non sia ottenuta solo a scapito di una minoranza etnica o sociale[32].

Una delle discriminanti da tenere in considerazione è quella che la sicurezza nazionale risponde a una minaccia che è potenzialmente mortale, al contrario una mancanza di privacy non comporta tali rischi. Questo è uno dei motivi per

---

technology: Towards a common framework for privacy and ethical assessment, ("Trade-offs and balancing" pp. 26-43) progetto PRESCIENT

[31] Diana Alonso Blas, 2009, *First Pillar and Third Pillar: Need for a Common Approach on Data Protection?* in S. Guthwirth e altri, Reinventing Data Protection?, Springer

[32] Chandler Jennifer, 2009, *Privacy versus national security: Clarifying the Trade-off*, in Kerr, Lucock e Steeves , Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Oxford University Press

cui uno Stato quando deve valutare il "costo opportunità" dell'uno o dell'altro potrebbe essere portato a dare la precedenza alla sicurezza nazionale sulla privacy.
Tuttavia, alcuni studiosi come Kevin Aquilina lamentano il fatto che il termine "sicurezza nazionale" è molto vago e ambiguo, e non di rado viene usato come copertura per motivare controverse azioni politiche[33].
Allo stato attuale una tecnologia che possa offrire sicurezza senza per forza dover sacrificare la privacy sembra inarrivabile e bisogna dunque trovare sempre il giusto bilanciamento. Persino una tecnologia come gli scanner ad onde millimetriche, che in linea teorica sembrano perfette per migliorare la sicurezza rispettando al tempo stesso privacy, ha i suoi piccoli limiti. In alcuni casi infatti vengono segnalati dei falsi positivi, e, per esempio, una persona con un pace maker sarà comunque costretta ad attraversare ulteriori controlli in una stanza di ispezione[34].

A causare interferenze e restrizioni nelle libertà dei cittadini non è solamente la sicurezza nazionale, ma anche la libertà di espressione. Szekely analizza proprio il possibile conflitto con la libertà d'espressione. Secondo questo autore i due termini non sono né amici, né nemici, bensì due concetti complementari di un gioco a somma zero[35].
Il suo ragionamento parte da una distinzione essenziale nel campo dei trattamenti dei dati, che possono essere distinti in due categorie: i dati prettamente personali, e i dati che possono essere di interesse pubblico. Per i primi dovrebbe prevalere il diritto alla privacy, mentre i secondi possono essere soggetti al diritto di informazione.

---

[33] Aquilina, Kevin, 2 marzo 2010, *Public security versus privacy in technology law: A balancing act?*, Computer Law & Security Review, Vol. 26, No. 2
[34] G. Valkenburg, 2014, *Privacy Versus Security: Problems and Possibilities for the Trade-Off Model* in S. Gutwirth e altri, Reforming European Data Protection Law, Law, Governance and Technology Series 20
[35] Ivan Szekely, 2009, *Freedom of Information Versus Privacy: Friends or Foes?* in Reinventing Data Protection?, Springer

Da questo punto di vista ha avuto un'importanza storica la sentenza della Corte Suprema americana nel caso New York Times contro Sullivan del 1964. Sullivan era un politico, il quale ritenendosi diffamato da un articolo del New York Times, citò il quotidiano a giudizio. Il tribunale però nella sua sentenza diede ragione al quotidiano, dichiarando per la prima volta nella storia che le figure pubbliche hanno meno diritto ad essere tutelati in quanto ciò che le riguarda è anche di interesse pubblico. Inoltre nella sentenza i giudici sostennero che il Primo Emendamento garantiva un diritto incondizionato di critica nei confronti delle figure pubbliche a garanzia della democrazia[36].

Szekely però va ad analizzare le figure pubbliche e pone un dilemma: quanto in là e quanto a lungo può spingersi il diritto d'informazione ad indagare nella vita privata di una figura pubblica? Una figura pubblica avrà sicuramente delle informazioni di pubblico interesse, ma d'altra parte avrà anche una vita privata che vorrà custodire con riservatezza. In una figura pubblica le due aree in parte si sovrappongono e certi aspetti della vita privata diventano rilevanti anche per il pubblico[37]. Quello che resta invece da stabilire è il giusto equilibrio, perché anche per una figura pubblica deve essere garantito un minimo rispetto della vita privata. Per esempio, nelle campagne elettorali americane viene richiesto ai candidati anche di rendere pubbliche le informazioni sulla salute. Diversamente, in Italia nessuno va a chiedere a un politico candidato le sue condizioni mediche, in quanto la sfera privata delle figure pubbliche viene considerata in questo caso con una maggiore ampiezza.

Inoltre il concetto di figura pubblica è dinamico, varia con gli anni, e al giorno d'oggi si è allargato a comprendere le categorie più disparate come quelle

[36] Decisione del 9 marzo 1964 della Corte Suprema degli USA nel caso New York Times Co. vs Sullivan

[37] Szekely, nota 35

degli sportivi, dei politici, delle persone dello spettacolo e molte altre[38].

1.4 Il terrorismo, l'era digitale e la fine della privacy?

Come emerso finora, la privacy costituisce un diritto fondamentale imprescindibile per la democrazia, che rappresenta al tempo stesso una garanzia per la tutela di altre libertà. Oggigiorno, tuttavia, ci sono due principali minacce per la privacy: una è rappresentata dalle pressioni per misure più stringenti per combattere il terrorismo, e l'altra dai cambiamenti allo stile di vita delle persone causati dalla rivoluzione digitale.

Già negli anni '90, agli albori dei progressi tecnologici, Scott McNealy, l'amministratore delegato di Sun Microsistems, analizzava gli inizi della rivoluzione digitale e guardando al futuro che si prospettava davanti all'umanità affermava: "*Voi avete zero privacy, rassegnatevi*[39]".

Nel 2010 toccava a Mark Zuckemberg, il creatore di Facebook, affermare che la privacy è una norma sociale che non esiste più[40]. Guardando le abitudini odierne di milioni di persone che caricano giornalmente sui social network foto e pensieri della loro vita ci sarebbe la tentazione di dargli anche ragione, ma se così fosse ciò sarebbe molto pericoloso.
Una mancanza di privacy è infatti una grave minaccia per le persone, e nel web i sui effetti si amplificano a dismisura, poiché ciò che viene caricato su

[38] Intervista a Stefano Rodotà del 12 marzo 2016 a Linkiesta, Consultabile su: http://www.linkiesta.it/it/article/2016/03/12/stefano-rodota-la-trasparenza-totale-e-unidea-da-dittatori/29592/
[39] Polly Sprenger, 26 gennaio 1999, *Sun on Privacy: 'Get Over It'*, Wired, Consultabile su: http://archive.wired.com/politics/law/news/1999/01/17538
[40] Bobbie Johnson, 11 gennaio 2010, *Privacy no longer a social norm, says Facebook founder*, Consultabile su: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

internet rimane lì per sempre.

Uno dei casi più famosi e citati, che dimostra chiaramente i pericoli della mancanza di privacy online e del fatto che il web non dimentica nulla, è la storia di Stacy Snyder. La Snyder è una cittadina statunitense alla quale venne negata l'abilitazione all'insegnamento. Nell'aprile 2006 l'allora studentessa venticinquenne aveva terminato gli esami e concluso il tirocinio con il massimo dei voti, tuttavia venne convocata dai funzionari dell'università e le fu riferito che non avrebbe potuto insegnare in quanto il suo comportamento non era conforme agli standard richiesti. I funzionari si riferivano ad una foto che la ragazza aveva caricato sul suo profilo Myspace. Nella foto era stata immortalata con un cappello da pirata, bevendo da un bicchiere di plastica e nella didascalia aveva scritto "*drunken pirate*" (pirata ubriaco). La foto fu notata da un'insegnante della scuola in cui la ragazza svolgeva il suo tirocinio e l'amministrazione della scuola fu allertata. La Snyder rimosse l'immagine dal suo profilo, tuttavia era ormai presente in modo definitivo negli indici dei motori di ricerca e nulla avrebbe più potuto cancellare ciò che era stato fatto. La Snyder provò a fare causa all'università, ma perse[41].

Internet, che avrebbe dovuto essere uno strumento attraverso il quale diffondere i valori della democrazia nel mondo rischia invece di avere un effetto inverso e costituire una riduzione delle libertà delle persone: rischia di diventare uno strumento di controllo, oltre a diventare uno strumento della discriminazione.

Ma quello dei social network è solo uno dei rischi alla privacy legati al mondo digitale. Al giorno d'oggi colossi informatici come Google vantano enormi profitto dalla vendita delle informazioni personali in pubblicità. Siamo entrati in un'era in cui "*i dati personali sono il nuovo petrolio di internet*

[41] Mayer-Schönberger, 2009, *Delete: The virtue of forgetting in the digital age*, Princeton: Princeton University Pres

e la nuova moneta del mondo digitale"[42].

Oggigiorno è diventata una consolidata realtà quella dei big: le nostre abitudini vengono tracciate, ogni nostra azione nel web viene registrata e catalogata, ed infine, attraverso la creazione di algoritmi sempre migliori, le aziende puntano addirittura a prevedere i comportamenti degli utenti, quasi a privarli della facoltà di scelta.

Purtroppo il web è nato senza limiti e restrizioni, si tratta ancora di un'area grigia ancora scarsamente regolamentata. L'abitudine a questa libertà fa sì che quando qualcuno cerca di fissare delle regole nasca subito una strenua opposizione. Eppure, come nel mondo reale gli uomini hanno abbandonato il caos, l'anarchia, lo stato di natura creando una società, uno Stato e delle regole per poter vivere in comune accordo, allo stesso modo è importante riuscire a raggiungere una legislazione condivisa anche a riguardo del mondo virtuale.

Per quanto riguarda il terrorismo bisogna rilevare che per molto tempo in Occidente tale parola era usata per riferirsi quasi esclusivamente a qualcosa di lontano, a delle politiche di efferata violenza che avevano luogo in regioni remote della terra. Era una minaccia che, per quanto riguarda l'Occidente, poteva colpire solo i militari impegnati in zone di guerra, ad esempio in Africa o in Medio Oriente. Tutto ciò è cambiato in seguito agli attentati alle Torri Gemelle dell'11 settembre 2001, che hanno portato il terrorismo alle porte di casa degli americani, sviluppando negli Stati Uniti una percezione di pericolo costante che si è infiltrata nella vite di milioni di persone, generando un profondo senso di insicurezza generale. La parola "terrorismo" cominciava ad occupare le prime pagine dei quotidiani, diventava un termine quotidiano che ha iniziato a occupare una parte sempre maggiore delle nostre esistenze. Il

[42] Kuneva M., 2009, *European consumer commissioner, keynote speech, roundtable on online data collection, targeting and profiling* (Brussels). Consultabile su: http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm.

terrorismo quel giorno è diventato una minaccia reale, che può colpire senza alcun preavviso la popolazione civile.
Volendo ridurre il rapporto tra privacy e sicurezza nazionale ad un semplicistico costo-opportunità, da quel momento in America il valore della sicurezza nazionale veniva percepito come estremamente più elevato delle libertà dei suoi cittadini.

Fu in quel frangente che l'allora Presidente degli Stati Uniti Bush diede avvio ad una guerra globale al terrorismo[43]. A partire da quel momento le politiche della sicurezza nazionale americana hanno avuto la precedenza e il sopravvento sulla tutela di altri diritti dell'uomo. La lotta al terrorismo globale ha dato avvio a una battaglia nella quale le agenzie di intelligence americana hanno avuto carta bianca e hanno iniziato ad usare qualunque metodo, lecito e non.

Nel 2013 le rivelazioni di Edward Snowden[44] hanno mostrato al mondo che gli Stati Uniti avevano iniziato un programma di sorveglianza di massa. Un programma che non riguardava solamente i cittadini americani, bensì sono state addirittura intercettate le comunicazioni di capi di Stato alleati e sono state spiate sedi dell'ONU e dell'Unione Europea[45].
Nell'operato dell'NSA vi è stata una totale mancanza dell'equilibrio che dovrebbe essere ricercato fra la necessità di incrementare la sicurezza e un rispetto alla privacy dei cittadini.

Il clamore provocato dalle rivelazioni di Snowden ha portato ad una revisione dell'NSA ed all'imposizione di maggiori limiti nell'operato delle

[43] Eric Schmitt e Thom Shanker, 26 luglio 2005, *U.S. Officials Retool Slogan for Terror War,* Consultabile su: http://www.nytimes.com/2005/07/26/politics/us-officials-retool-slogan-for-terror-war.html
[44] ex consulente della NSA, la National Security Agency
[45] Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark, 29 giugno 2013, *NSA Spied on European Union Offices*, Der Spiegel Consultabile su: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

agenzie di intelligence[46].

La paura e la necessità di sicurezza non devono però portare ad eccessi come quelli avvenuti negli Stati Uniti e per ogni decisione presa deve essere valutato attentamente quale impatto avrà sulle libertà fondamentali dei cittadini. La lotta al terrorismo dovrebbe anche rappresentare una lotta tra valori e ideologie diverse. In quest'ottica è particolarmente importante che non venga svenduta la privacy degli individui, perché rinunciare alla privacy vorrebbe dire una sconfitta dei valori della democrazia e per il mondo libero.

[46] In particolare con l'approvazione dell'USA Freedom Act il 2 giugno 2015, che sostituiva il Patriot Act, viene proibita la raccolta di dati di massa

Capitolo 2
I principali strumenti legislative a tutela del diritto alla protezione dei dati personali

2.1 L'Europa come principale promotore del diritto alla privacy: la CEDU

L' Europa è il luogo per eccellenza dove si ha avuto e si ha la promozione della protezione dei dati personali.

Indubbiamente sono state le tragiche esperienze dei regimi totalitari nella prima metà del Novecento a sviluppare a consolidare nella mentalità europea il valore che deve essere attribuito ad una tutela della sfera privata delle persone.

Dopo aver vissuto un periodo buio in cui la censura, le leggi razziali e altre politiche repressive erano la quotidianità per milioni di persone, veniva avvertito ovunque il bisogno di proteggere l'individuo e le sue libertà, e di evitare che simili orrori e sciagure potessero ripetersi nella storia.

In un primo tempo la spinta per la promozione del diritto alla privacy è stata infusa dall' importantissimo lavoro del Consiglio d'Europa, un'organizzazione regionale a vocazione universale, nata dalle ceneri della seconda Guerra Mondiale.

Nel 1950, all'interno del Consiglio d'Europa venne firmata a Roma che nel 1953 gli stati allora membri raggiunsero l'accordo per firmare la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

(da qui in avanti “CEDU”)[47].

La CEDU rappresenta il primo trattato che mira alla tutela dell’individuo e ancora oggi l’unico dotato di un meccanismo giurisdizionale permanente di garanzia, al quale ogni persona può richiedere la salvaguardia dei diritti garantiti dalla Convenzione[48].

Particolarmente rilevante ai fini dell’argomento qui trattato è in particolare l’articolo 8 sul diritto al rispetto della vita privata e familiare:

1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.

2. Non può esservi ingerenza di una autorità pubblica nell’esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell’ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui.

Nel primo comma troviamo un ambito di applicazione molto vasto di protezione dei diritti dell’individuo che può andare dal diritto al nome al all’autonomia personale, passando per la tutela della riservatezza. Nel secondo comma viene vietata l’ingerenza di autorità pubbliche, limitandola a casi eccezionali quali ordine pubblico e sicurezza nazionale.

Nel momento in cui si è diffusa una gestione automatizzata dei dati, la maggior quantità di informazioni in circolazioni ha posto in primo piano la questione della protezione dei dati personali, evolvendo ulteriormente

[47] la Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali è stata firmata a Roma il 4 Novembre 1950 ed è entrata in vigore il 3 settembre 1953 in seguito al deposito di almeno dieci strumenti di ratifica. Per l’Italia è entrata in vigore solamente a partire dal 10 ottobre 1955 in seguito alla ratifica con legge n. 848 del 4 agosto 1955, e successiva pubblicazione in Gazzetta Ufficiale n. 221 del 24 settembre 1955. Sono oggi parte del trattato tutti e 47 i paesi membri del Consiglio d’Europa.

[48] P. Gianniti, 2015, *La CEDU e il ruolo delle corti*, Zanichelli

l'ambito di riservatezza dell'individuo ed il concetto di privacy.

Si tratta delle fondamenta da cui poi sono successivamente scaturiti ulteriori trattatati sulla protezione dei dati personali.

2.2 L'evoluzione dell'articolo 8 nelle sentenze della Corte EDU

L'articolo 8 è stato meglio definito in seguito alle sentenze della Corte europea dei diritti dell'uomo (Corte EDU).

Guardando ad esempio l'estensione del concetto di "dati personali", questo contiene al suo interno ben più delle semplici generalità, ma anche ad esempio impronte digitali e DNA.

Al riguardo basta prendere in esame la pronuncia della sentenza nei casi *S. e Marper contro il Regno Unito*.[49]

Nel gennaio 2001 S. fu arrestato all'età di 11 anni per tentata rapina. Furono raccolte le sue impronte digitali e un campione del suo DNA. Vene poi assolto il 14 giugno 2001. Nel marzo 2001 il signor Marper venne arrestato con l'accusa di molestie nei confronti del partner. Anche in questo caso furono raccolte impronte digitali e campioni di DNA. Il caso venne poi chiuso il 14 giugno in seguito alla riconciliazione con il partner. Entrambi una volta scagionati dalle accuse fecero richiesta perché le impronte digitali, i campioni di DNA e i profili fossero distrutti. La richiesta non venne accolta in quanto la legge autorizzava una conservazione dei dati a tempo indeterminato. I due fecero fecero allora ricorso alla Corte EDU.

Nella sua decisione la Corte notava che i campioni biologici potevano fornire molte informazioni sensibili su un individuo, tra cui informazioni sul suo stato

[49] Sentenza della Corte EDU del 4 dicembre 2008 nei casi *S. e Marper contro il Regno Unito*

di salute. La conservazione dei campioni biologici rappresentavano di per sé una violazione del diritto al rispetto della vita privata degli individui. Inoltre anche le possibilità di derivare dal DNA dei dati personali unici, che possono essere usati per costruire relazioni genetiche tra gli individui, interferisce con la tutela della loro sfera privata. In particolar modo, la possibilità di ricavare dal DNA le origini etniche di un individuo rendono la sua consernvazione ancor più suscettibile di danneggiare la vita privata di un individuo. La Corte al riguardo concluse che la conservazione di campioni biologici e DNA interferisce con il rispetto della vita privata, garantito dall'articolo 8 della CEDU[50].

Le impronte digitali contengono invece una minor quantità di informazioni rispetto a DNA e campioni biologici, tuttavia la loro conservazione viene valutata come un' eguale ingerenza nella vita privata[51].

La Corte rilevò che l'uso di nuove tecnologie non può essere consentito a tutti i costi, senza una valutazione della proporzionalità tra i benefici di un uso estensivo di tali tecnologie e la loro ingerenza nella privacy degli individui.

A maggior ragione in questa vicenda va tenuto anche conto del fatto che i due ricorrenti non erano stati incriminati, bensì scagionati dalle accuse, e inolte uno dei due era minorenne, rendendo il suo caso ancora più delicato.

La Corte aveva dunque valutato che la conservazione di campioni biologici, DNA e impronte digiatali di individui sospettati, ma non incriminati, manca della giusta proporzionalità tra l'interesse pubblico e il rispetto della sfera privata dell'individuo e non può essere ritenuta necessaria in una società democratica[52].

L'articolo 8 vuole anche tutelare informazioni personali che non dovrebbero essere pubblicate senza il consenso dell'interessato.

[50] *S. e Marper contro il Regno Unito* nota 49 (punti 72:77)
[51] *S. e Marper contro il Regno Unito* nota 49 (punto 86)
[52] *S. e Marper contro il Regno Unito* nota 49 (punto 125-126)

È stato questo al centro del caso *Alkaya contro Turchia*[53].
In seguito ad un furto a casa di una nota attrice turca un quotidiano nazionale scrisse un articolo sull'effrazione nel quale riportava anche l'indirizzo esatto dell'abitazione. L'attrice chiese i danni al quotidiano, ma la richiesta non venne accolta dalla corte domestica.
L'indirizzo di residenza di una persona è un'informazione prettamente personale e dunque viene tutelata dall'articolo 8 della CEDU. Dall'altra parte il quotidiano basava la sua difesa sull'articolo 10 della medesima Comvenzione, cioè la garanzia della libertà di espressione.
La Corte EDU doveva dunque decidere quale fosse il giusto rapporto tra diritto alla privacy e libertà di espressione e in questo caso l'elemento decisivo per formulare una valutazione era costituito dal contributo all'interesse pubblico apportato da tali informazioni. In questo caso la Corte valutò che non vi erano ragioni di pubblico interesse per pubblicare l'indirizzo dell'attrice, sebbene costei fosse una "figura pubblica". Inoltre, pubblicare tale informazione poteva avere ripercussioni negative sulla sicurezza del soggetto, oltre che sulla sua vita privata.[54]

Oltre alla pubblicazione di un indirizzo anche menzionare per intero il nome di una persona costituisce un'ingerenza al rispetto della vita privata di un individuo.
Nel caso *Kurier Zeitungsverlag e Druckerei GmbH contro Austria* due editori austriaci si rivolsero alla Corte EDU per una presunta violazione dell'articolo 10 da parte dei giudici nazionali[55].
I due avevano pubblicato alcuni articoli sulla disputa di una coppia per l'affidamento di un minore. Negli articoli erano contenute informazioni

[53] Sentenza della Corte EDU del 9 ottobre 2012 nel caso *Alkaya contro Turchia*
[54] *Alkaya contro Turchia* nota 53
[55] Sentenza della Corte EDU del 19 giugno 2012 nel caso *Kurier Zeitungsverlag e Druckerei GmbH contro Austria*

sull'identità del minore, dettagli della sua vita familiare e foto che lo ritraevano in condizioni di sofferenza.
La madre e il figlio avevano poi citato a giudizio i due editori, chiedendo un risarcimento per l'ingerenza nella vita del bambino e la Corte regionale di Vienna diede loro ragione.
A quel punto gli editori si rivolsero alla Corte EDU, ritenendo che quella sentenza violasse la loro libertà di espressione.
La Corte EDU si ritrovava dunque valutare se l'ingerenze compiuta dai due editore potesse essere ritenuta "necessaria in una società democratica" sulla base della libertà di espressione.
La Corte dichiarò che in generale le fotografie servono per soddisfare la curiosità dei lettori su certi argomenti di interesse generale o raffiguranti personaggi pubblici[56].
La Corte analizzando il caso rilevò però che il soggetto in questione non era una figura pubblica, né era diventato parte di una vicenda di interesse pubblico. L'articolo aveva dato vita ad un dibattico pubblico, ma per i suoi fini non era necessario rivelare informazioni sull'identità del bambino. Il bambino era vittima della vicenda e non era entrato di sua intenzione nella sfera pubblica. Proprio per la sua vulnerabile posizione di minore doveva anzi essere maggiormente tutelato[57].
La Corte rifiutò dunque la richiesta dei due editori, valutando che l'ingerenza nella loro libertà di espressione era più che giustificata e proporzionata ai fini di proteggere la privacy del minore.

La sentenza *Copland contro il Regno Unito* specificò che la vita privata include non solo la privacy delle telefonate ma anche la riservatezza delle e-mail, e dell'uso di Internet[58].

[56] *Kurier Zeitungsverlag e Druckerei GmbH contro Austria* nota 55 (punto 50)
[57] *Kurier Zeitungsverlag e Druckerei GmbH contro Austria* nota 55 (punto 59)
[58] Sentenza della Corte EDU del 3 aprile 2007 nel caso *Copland contro il Regno Unito*

La signora Copland lavorava come assistente personale in un college scozzese. Per sei mesi le sue telefonate, la cronologia della sua navigazione web e le sue e-mail furono monitorate dall'università.
L'università giustificò le sue azioni con due scuse: la prima riguardava la protezione dei diritti e delle libertà degli altri, assicurandosi che le strutture non fossero usate per scopi personali, e in secondo luogo l'università riteva di poter esercitare un ragionevole controllo sulle sue strutture e di fare quanto necessario per proveddere a garantire un'istruzione di elevato livello.
La Corte EDU doveva quindi valutare se l'ingerenza nel diritto alla privacy era giustificabile o no.
La Corte dichiarò che come era già stato affermato nella sentenza Halford contro Regno Unito che controllare le chiamate è un'azione protetta dall'articolo 8 della CEDU a prescindere che ciò avvenga sul luogo di lavoro.
La Corte poi ritenne che la sorveglianza applicata a e-mail e internet doveva essere trattata allo stesso modo delle chiamate[59].
L'articolo 8 venne dunque espanso dalla sentenza a protezione della corrsipondenza non solo domestica, ma anche sul luogo di lavoro.

Sono poi senz'altro protetti i dati personali riguardanti la salute di un individuo come ha osservato la Corte nella sentenza del caso *Z. contro Finlandia*[60].
In caso ha origine in seguito al fatto che una sentenza di una Corte d'appello finlandese rende pubbliche l'identità della moglie del condannato e la sua sieropositività.
La pubblicazione di tali informazioni aveva violato il rispetto della vita privata e familiare della donna.
La Corte aggiunse che il rispetto della confidenzialità dei dati personali sulla

[59] *Copland contro il Regno Unito* nota 58 (punto 41)
[60] Sentenza della Corte EDU del 25 febbraio 1997 nel caso *Z. contro Finlandia*

salute è un principio essenziale nei sistemi legali di tutti gli Stati parte della Convenzione. Non solo bisogna rispettare il suo diritto alla privacy, ma è necessario garantire la sua fiducia nel sistema sanitario. Le leggi nazionali devono dunque prevedere delle tutele verso i dati personali sulla salute per impedire che possano essere comunicati o rivealti.

L'articolo 8 della CEDU contiene inoltre delle obblighi positivi a carico degli Stati a garantire il rispetto dei diritti dell'articolo, nonostante questo sia fondamentalmente scritto al negativo.
Uno dei primi casa a dimostrare che vi possono essere obblighi positivi per lo Stato a protezione dei diritti della riservatezza fu la vicenda *Airey contro Irlanda*[61].
La signora Airey chiedeva che per il rispetto della vita familiare le fosse garantita un aiuto legale per la causa di separazione.
La donna voleva ottenere una separazione dal marito violento. Tuttavia non poteva raggiungere un accordo con il marito, ma non aveva neppure i mezzi finanziari per potersi rivolgere a un avvocato.
La donna si rivolse allora alla Corte EDU ritenendo che vi fosse stata una violazione dell'articolo 6, riguardo al suo diritto di accedere ad una corte.
La Corte dichiarò che molti diritti hanno implicazioni economiche e sociali che portano a obblighi positivi. In particolare in questo caso vi era un diritto di assistenza legale per poter effettivamente accedere al tribunale. Secondo la Corte EDU la donna non poteva accedere in modo efficace alla Irish High Court (Alta Corte Irlandese) in quanto le procedure erano complesse e vi era inoltre la possibilità che il marito potesse essere rappresentato da un avvocato. La Corte aggiunse che anche l'articolo 8 del rispetto della vita familiar era stato violato. Il diritto alla vita familiare poteva contenere degli obblighi positivi per accedere a meccanismi di protezione della vita familiare,

[61] Sentenza della Corte EDU del 9 ottobre 1979 nel caso *Airey contro Irlanda*

e come nel caso in questione, la capacità di poter procedere ad una separazione.

In un caso più recente sono anche messe in evidenza gli obblighi positivi nel contesto di Internet: la vicenda *K.U. contro Finlandia*[62].
Nel 1999 un individuo sconosciuto pubblicò un'inserzione in un sito di dating utilizzando il nome e altre informazioni del ricorrente, che a quel tempo aveva 12 anni. Quest'ultimo divenne consapevole di ciò che gli era capitato quando ricevette una e-mail da un uomo sconosciuto.
Il padre del ricorrente chiese alla polizia di identificare la persona che aveva pubblicato l'annuncio a nome del figlio, tuttavia il provider di internet si rifiutò di rilasciare quelle informazioni alla polizia, in quanto si riteneva vincolato dalla confidenzilità delle telecomunicazioni secondo la legge finlandese.
Il 19 gennaio 2001 anche la Corte distrettuale di Helsinki rifiutò la richiesta della polizia di obbligare il provider di internet a fornire l'identità dell'uomo che aveva pubblicato l'inserzione.
Il caso venne poi preso in carico dalla Corte EDU il 27 giugno 2006.
La Corte rilevò che l'azione di pubblicare un'inserzione a nome del ricorrente era stata un'azione criminale, che aveva reso il minore un obiettivo di pedofili. I minori e altri individui vulnerabili devono ricevere dallo Stato protezione contro interferenze nella loro vita privata[63].
Secondo la Corte nel 1999 era già chiaro che la rete poteva essere usata per fini criminali e dunque il Governo finlandese aveva colpa di non aver messo in atto dei meccanismi di protezione. La normativa dovreva essere in grado di soppesare da una parte la confidenzialità del servizio Internet e dall'altra l'importanza della prevenzione dei crimini e la protezione dei diritti e delle libertà degli individui[64].

[62] Senteza della Corte EDU del 2 dicembre 2008 nel caso *K.U. v. Finland*
[63] *K.U. v. Finland* nota 62 (punti 40-41)
[64] *K.U. v. Finland* nota 62 (punti 48-49)

La Corte ritenne dunque che la Finlandia era venuta meno al suo dovere di proteggere la vita privata del ricorrente, poiché era stata data la precedenza alla confidenzialità rispetto al benessere psico-fisico della vittima. Vi era dunque stata una violazione dell'articolo 8.

Un'altra sentenza che è stata essenziale per lo sviluppo dell'articolo 8 della CEDU, fu quella del caso *Leander contro Svezia* del marzo 1987[65].
Il caso riguardava un carpentiere svedese che desiderava lavorare in un museo adiacente ad un'area militare ad accesso ristretto. La sua applicazione per il posto di lavoro gli venne però rifiutata durante le procedure di selezione del personale sulla base di alcuni file segreti della polizia. Il ricorrente chiese di accedere ai file ma gli fu negato.
La Corte ritenne che l'uso di file segreti della polizia e il susseguente rifiuto a consentire l'accesso a tali informazioni costituisse un'ingerenza nel diritto alla vita privata del soggetto e quindi una violazione dell'articolo 8.
Il giudizio in questione è di particolare importanza perché viene dichiarato che anche la sola conservazione di dati personali costituisce una violazione dell'articolo 8, a prescindere da un possibile utilizzo o meno di tali dati[66].
Nonostante la violazione dell'articolo 8, la Corte valutò infine che nel caso in questione tale violazione era giustificata da motivi di sicurezza nazionale.

Un ulteriore sentenza a ribadire ciò arriva con il caso *Amann contro Svizzera*[67].
Il caso riguardava una telefonata ricevuta dal ricorrente, effettuata dall'interno dell'ambasciata sovietica per ordinare delle strisce depilatorie pubblicizzate dal ricorrente. La chiamata fu intercettata e fu chiesto ai servizi segreti di scrivere un file sul ricorrente.

[65] Sentenza della Corte EDU del 26 marzo 1987 nel caso *Leander contro Svezia*
[66] *Leander contro Svezia* nota 65 (punto 48)
[67] Sentenza della Corte EDU del 16 febbraio 2000 nel caso *Amann contro Svizzera*

La Corte valutò quell'azione come una violazione dell'articolo 8 della CEDU per quanto riguarda la registrazione della telefonata, e la creazione e conservazione di un file sul ricorrente.
Queste violazioni non potevano inoltre ritenersi in accordo con la legge Svizzera e neppure necessarie in una società democratica.

Diverso fu invece l'esito del caso della vicenda *Uzun contro Germania*[68]. Nell'ottobre 1995 venne aperta un'indagine contro il ricorrente, il signor Uzun, un cittadino tedesco presunto complice di alcune esplosioni causate dalla cellula anti-imperialista (Antiimperialistische Zelle).
Ai fini delle indagini fu autorizzata una sorveglianza del signor Uzun, nonché una videosorveglianza del suo edificio, l'ascolto delle chiamate e l'installazione di cimici nell'auto di un presunto complice.
I due uomini trovarono e distrussero le cimici e a quell punto il procuratore generale ordinò l'utilizzo di installare una ricetrasmittente GPS per localizzare la posizione della sua auto. La sorveglianza iniziata nel dicembre 1995 terminò con l'arresto dei due uomini nel febbraio 1996.
Il signor Uzun fu condannato a 13 anni di prigione per tentato omicidio.
Grazie anche alle informazioni ottenute dalla sorveglianza GPS fu scoperto che i due uomini avevano posizionato varie bombe di fronte alle abitazioni di membri del Parlamento e un consolato.
Il signor Uzun fece ricorso contro l'uso del GPS, ma la Corte federale di giustizia (Bundesgerichtshof) rigettò il caso.
Si presentò successivamente di fronte alla Corte federale costituzionale (Bundesverfassungsgericht), ma quest'ultima dichiarò che la misura di sorveglianza aveva causato un'ingerenza nella vita sua privata, che era proporzionata alla gravità delle sue azioni e al fatto che avesse eluso altre misure di sorveglianza.

[68] Sentenza della Corte EDU del 2 settembre 2010 nel caso *Uzun contro Germania*

In ultima battuta si presento alla Corte EDU lamentando che la sorveglianza GPS era stata una violazione dell'articolo 8 della CEDU.
La Corte in primis dichiarò che il controllo dei movimenti di una persona attraverso il monitoraggio della sua posizione GPS costituiva un'ingerenza con il diritto al rispetto della sua vita privata[69].
Tuttavia la Corte poi valutò che la sorveglianza GPS era stata attuata in accordo con la legge tedesca. In più, in base a tele legge, i requisiti per autorizzare una sorveglianza GPS sono elevati e può essere attuata solo nei confronti di sospettati di crimini di una certa entità.
La sorveglianza GPS non poteva essere attivata in modo arbitrario, bensì richiedeva un controllo giudiziario. Erano dunque previste sufficienti protezioni contro eventuali abusi di tale controllo. In base al giudizio della Corte, l'ingerenza nella vita privata del signor Uzun era avvenuta in accordo con la legge tedesca[70].
In più la Corte notava che le misure di sorveglianza erano state adottate per salvaguardare la sicurezza pubblica, in quanto il soggetto era ritenuto responsabile di innumeroveli tentati omicidi come membro di un'organizzazione terroristica. Inoltre, tali intrusive misure erano state messe in atto solo dopo che altri metodi si erano rivelati insufficienti.
Considerata la gravità dei crimini le misure erano da ritenersi proporzionate e necessarie in una società democratica, e la Corte si pronunciò unanime nel ritenere non vi fosse stata alcuna violazione dell'articolo 8[71].

La Corte si è ritrovata ad esaminare l'articolo 8 in relazione ad un diritto di accesso a dati conservati dallo Stato, come nella vicenda *Gaskin contro Regno Unito*[72].

[69] *Uzun contro Germania* nota 68 (punto 52)
[70] *Uzun contro Germania* nota 68 (punto 73)
[71] *Uzun contro Germania* nota 68 (punti 78,79,80)
[72] Sentenza della Corte EDU del 2 settembre 2010 nel caso *Gaskin contro Regno Unito*

Il ricorrente era un orfano che aveva trascorso una travagliata e sofferta infanzia durante la quale era stato costretto a vivere presso diverse famiglie. Diventato maggiorenne il signor Gaskin desiderava poter scavare nel suo passato per riuscire a superare i traumi che gli erano stati provocati e che ancora lo tormentavano.
Fece così domanda ai servizi sociali che si erano occupati della sua pratica, di poter visionare il suo dossier, per scoprire in quali famiglie aveva risieduto per poterle così contattare per far luce sul suo passato e tentare così di superare i suoi problemi. L'accesso al dossier gli fu rifiutato, in quanto i servizi sociali si ritenevano vincolati dalla confidenzialità del rapporto.
A quel punto fece richiesta alla Corte d'appello, la quale però rigettò la richiesta, in quanto essa non costituiva un interesse pubblico. Rivelare le informazioni del dossier avrebbe rivelato informazioni strettamente confidenziali.
Il passo successivo fu allora quello di presentarsi alla Corte EDU.
La Corte trovò nello Stato un'obbligo positivo affinché un individuo possa accedere alle informazioni che riguardano la sua vita. Il caso infatti differeva da molti altri in cui la questione era sulla legittimità della raccolta e conservazione di alcuni dati. A tal riguardo il signor Gaskin non muoveva alcuna accusa, ciò che invece voleva ottenere era l'accesso a tali dati personali.
Secondo il governo inglese però tali dati contenuti nei dossier dei servizi sociali non potevano essere ritenuti parte della sua vita privata e familiare, in quanto costituito da dati raccolti dalle autorità locali[73].
La Corte valutò che per il ricorrente l'accesso al dossier costituiva un interesse di vitale importanza, che rientrava nelle sfere di protezione della Convenzione.

[73] *Gaskin contro Regno Unito* nota 72 (punto 35)

D'altra parte la Corte riteneva anche che la confidenzialità di registri pubblici fosse di fondamentale importanza al fine di garantire informazioni oggettive ed affidabili, e dunque la confidenzialità poteva essere necessaria per proteggere dei terzi[74].
Nel caso in questione però non era possibile chiedere il consenso agli informatori anonimi che avevano contribuito alla redazione del dossier e doveva dunque essere posta nelle mani di un'autorità indipendente la decisione di far accedere il ricorrente alle informazioni della sua infanzia.
Non essendo però stata messa in atto alcuna procedura del genere, il Regno Unito era venuto meno ad un suo obbligo positivo nei confronti del signor Gaskin, causando così una violazione dell'articolo 8[75].

Un successivo caso riguardante il diritto all'accesso dei dati, contenuto all'interno dell'articolo 8 fu quello *Haralambie contro Romania*[76].
Il signor Haralambie è un cittadino rumeno che riteneva di continuare a subire le conseguenze di alcune persecuzioni che aveva subito durante il regime comunista. In quel tempo confische di alcune terre.
Fece richiesta ad una corte per riappropiarsi delle terre che un tempo gli appartenevano, ma questa fu rigettata dal tribunale.
A quel punto richiese di accedere al dossier che era stato compilato su di lui dai precedenti servizi segreti del regime comunista. Dovettero passare sei anni prima che gli fosse concesso di accedere a tale dossier.
Nel frattempo nel 2003 aveva adito la Corte EDU.
La Corte ritenne che per il ricorrente accedere al dossier che lo riguardava era di vitale importanza e le autorità avevano un dovere affinché questi potesse accedere alle informazioni che vi erano contenute.

[74] *Gaskin contro Regno Unito* nota 72 (punti 41:44)
[75] *Gaskin contro Regno Unito* nota 72 (punto 49)
[76] Sentenza della Corte EDU del 27 ottobre 2009 nel caso *Haralambie contro Romania*

Gli ostacoli che il ricorrente aveva trovato nell'accedere alle informazioni che lo riguardavano costituivano per la Corte una violazione dell'articolo 8. Né la quantità di file, né eventuali disfunzioni dell'archivio potevano in alcun modo costituire una giustificazione per i sei anni di attesa che il ricorrente aveva dovuto aspettare per visionare le informazioni.

L'applicazione dell'articolo 8 venne anche estesa ai dati visivi ottenuti da videosorveglianze, in seguito alla sentenza *Peck contro Regno Unito*[77].
Il ricorrente era stato filmato da alcune telecamere a circuito chiuso in una strada pubblica, alcuni momenti dopo aver tentato il suicidio incidendosi il polso con un coltello da cucina. Alcuni mesi dopo i filmati registrati furono utilizzati per sponsorizzare i benefici dell'utilizzo di sistemi di videosorveglianza a circuito chiuso. In tali filmati il viso del ricorrente era facilemente riconoscibile e solamente in versioni successive la sua identità venne protetta.
Dopo che le richieste del ricorrente furono respinte della Corte d'appello, in quanto le autorità giudiziarie non ritenevano che la diffusione di tale materiale potesse costituire una violazione dell'articolo 8. L'uomo si presentò allora alla Corte EDU.
La Corte giudicò l'utilizzo di tali registrazione come un'ingerenza sproporzionata e ingiustificata della vita privata del ricorrente, priva di sufficiente tutela e dunque una violazione dell'articolo 8.
Il ricorrente si trovava in una strada pubblica tuttavia non si trovava là per partecipare ad un evento pubblico o come figura pubblica.
Da una parte la Corte riconobbe che i sistemi di videosorveglianza a circuito chiuso costituiscono un importante strumento per individuare e prevenire il crimine e che il suo utilizzo era reso più efficace attraverso la

[77] Sentenza della Corte EDU del 28 gennaio 2003 nel caso *Peck contro Regno Unito*

pubblicizzazione di quel sistema[78]. Dall'altra parte la Corte notò che avrebbe dovuto ottenere il consenso del ricorrente prima di rilasciare il video, e inoltre avrebbe potuto mascherarne l'identità o assicurarsi che i media a cui fornì il filmato prendessero precauzioni per tutelare la sua identità[79].
La Corte valutò infine una violazione dell'articolo 13, diritto ad un ricorso effettivo e dell'articolo 8, cioè di un'ingerenza ingiustificata nella sua vita privata.

Inoltre l'articolo 8 comprende al suo interno anche la protezione dell'immagine, come è stato dichiarato dalla sentenza *Von Hannover contro Germania*[80].
Nel caso in esame la principessa Von Hannover tentava di proteggere la sua privacy dalle continue intrusioni dei paparazzi.
In più di un'occasione la principessa provò a intentare delle cause contro i quotidiani che pubblicavano foto di momenti privati della sua vita, tuttavia le corti tedesche ritenevano che in quanto figura pubblica doveva tollerare le ingerenze nella sua vita privata.
Di diverso avviso fu invece il giudizio della Corte EDU, che ha ritenuto le sentenze delle corti tedesche abbiano costituito un'ingerenza nel diritto al rispetto della sua vita privata.
La pubblicazione di foto della sua vita quotidiana, sia da sola, sia in compagnia, ricadono all'interno della protezione garantita dall'articolo 8 e tale protezione non viene meno se sono presenti anche terzi.
La Corte dichiarò che sebbene la libertà di espressione si estenda anche alla pubblicazione di foto, quella è tuttavia un'area in cui la protezione dei diritti e della reputazione altrui è di estrema importanza.

[78] *Peck contro Regno Unito* nota 77 (punto 79)
[79] *Peck contro Regno Unito* nota 77 (punto 80:85)
[80] Sentenza della Corte EDU del 24 giugno 2004 nel caso *Von Hannover contro Germania*

Inoltre le immagini contengono “informazioni” molto personali e molto intime riguardo ad un individuo. In più le foto che appaiono nelle riviste sono spesso ottenute in modo molto molesto, che porta la persona a sentire una pesante intrusione nella sua vita privata.
La Corte quindi analizzò che l’articolo 8 serve a proteggere l’individuo da possibili intrusioni arbitrarie delle autorità pubbliche, ma a questo diritto negativo si può aggiungere anche un obbligo positivo per garantire l’effettivo rispetto della vita privata o familiare. Questi obblighi possono anche contemplare misure per assicurare il rispetto della vita privata tra individui[81].
Infine, il fattore determinante deve essere il rapporto tra il diritto di espressione e quello di tutela della vita privata, e quanto le foto possano contribuire ad un argomento di pubblico interesse.
Nel caso della principessa Von Hannover, quando costei non esercita funzioni pubbliche presenziando eventi, ciò che fa non può essere ritenuto di interesse pubblico in una democrazia. La stampa si limita a soddisfare la curiosità di un particolare frangia di lettori. La libertà di espressione va dunque intesa in modo più limitato, a garanzia del diritto alla vita privata[82].

Riguardo alle intercettazioni una discriminante importante per valutare la loro ingerenza è la presenza di leggi nazionali che ne impediscano un uso indiscriminato, come si può dedurre dalla sentenza del caso *Taylor-Sabori contro Regno Unito*[83].
Il ricorrente del caso in questione fu sorvegliato dalla polizia tra l’agosto 1995 e l’arresto del ricorrente nel gennaio 1996. La polizia fun infatti capace di intercettare tutti i messagg che riceveva nel cercapersone.
Dopo essere stato arrestato ed incriminato ad una reclusione di dieci anni per traffico di droga.

[81] *Von Hannover contro Germania* nota 80 (punto 57)
[82] *Von Hannover contro Germania* nota 80 (punto 65)
[83] Sentenza della Corte EDU del 22 gennaio 2003 nel caso *Taylor-Sabori contro Regno Unito*

Il ricorrente si appellò contro la condanna e la sua difesa si basava sulla non ammissibilità delle prove ottenute dal cercapersone. I giudici tuttavia rigettarono l'appello, ritenendo le prove ammissibili anche senza un mandato. La Corte EDU nell'analizzare il caso notò che al tempo degli eventi il Regno Unito non aveva un sistema che regolamentasse l'intercettazioni dei messaggi dei cercapersone e dunque l'ingerenza non si accordava con la legge e costituiva una violazione dell'articolo 8 della CEDU.

In modo simile al caso appena descritto la Corte EDU ha valutato un caso più recente fra *Roman Zakharov contro Russia*[84].
Il caso riguarda un sistema di intercettazione segreta delle comunicazioni nei cellulari russi. Il ricorrente è l'editore di una rivista che lamenta che gli operatori telefonici russi devo preinstallare per legge nei cellulari sei software che permettono alle agenzie di sicurezza di accedere ai dispositivi ed effettuare intercettazioni senza alcuna protezione per gli utenti.
La Corte EDU diede ragione all'editore, ritenendo che tale pratica costituisce una violazione dell'articolo 8 della CEDU.
In base alle analisi della Corte il sistema normativo russo non dava sufficienti garanzie da un utilizzo arbitrario dei sistemi di intercettazione e dal rischio di abusi connaturato ad un sistema di sorveglianza segreta. Un rischio che in Russia era particolarmente alto in quanto la polizia e i servizi segreti avevano i mezzi tecnici per accedere direttamente a tutte le comunicazioni mobili.
La Corte valutò carente in particolare alcuni aspetti: quali fossero le circostanze in cui i servizi segreti potevano accedere a misure di sorveglianza segrete; la durata di tali misure e in quali casi vi debba essere posto termine, quali siano le procedure per autorizzare le intercettazioni e quelle per la loro conservazione ed infine distruzione; e la mancanza di una supervisione di tali intercettazioni. Inoltre la possibilità di fare ricorso contro le intercettazioni era

[84] Sentenza della Corte EDU del 4 dicembre 2015 nel caso *Roman Zakharov contro Russia*

vincolata dalla necessità di portare prove delle intercettazioni, e ottenere tali prove era di fatto impossibile per via di una mancanza di un sistema di notifica dell'intercettazione in corso e dell'impossibilità di accedere a informazioni che riguardino le intercettazioni.

Inifine un caso riguardante la conservazione di dati personali su registri criminali è quello di *M.M. contro Regno Unito*[85].
Nel 2000 la ricorrente fu arrestata dopo essere scomparsa per un giorno con il nipote nel tentativo di evitare la sua partenza per l'Australia in seguito alla separazione avvenuta nel matrimonio del figlio.
Le autorità decisero di non perseguire penalmente la donna ma di limitarsi ad una diffida che sarebbe dovuta rimanere nei registri per cinque anni, ma poiché la parte danneggiata era un minore fu estesa a tempo indefinito.
Nel 2006 aveva ricevuto un'offerta di lavoro ma in seguito ad un controllo dei registri criminali tale offerta venne ritirata.
La Corte EDU valutando il caso trovò una violazione dell'articolo 8.
Nel sistema dei registri delle attività criminali non vi erano sufficienti tutele per la conservazione e l'accesso a i dati lì contenuti.
In particolare la conservazione dei dati ne permetteva l'accesso pubblico anche in un momento molto distante dall'evento, quando chiunque avrebbe già scordato quell'accaduto, soprattutto nel caso in questione dove la diffida era avvenuta in privata. Come la diffida diventa un elemento del passato, allo stesso tempo diventa parte della vita privata di una persona che deve essere rispettata.

[85] Sentenza della Corte EDU del 13 novembre 2012 nel caso *M.M. contro Regno Unito*

2.3 La Convenzione di Strasburgo n. 108

Un successiovo importante passo in avanti fu svolto sempre in sede del Consiglio d'Europa nel 1981. Quell'anno vennero infatti conclusi i lavori che portarono all'apertura alla firma della Convenzione di Strasburgo n.108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale (da qui in avanti "Convenzione 108")[86], un trattato internazionale giuridicamente vincolante a riguardo della protezione dei dati personali.

Nel preambolo viene infatti fatta presente la necessità di "*estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica*".

La Convenzione è entrata in vigore per i 47 Stati membri del Consiglio d'Europa ed è inoltre stata ratificata ed entrata in vigore per Mauritius e Uruguay e dovrebbero prossimamente aderirvi Capo Verde, Marocco, Senegal e Tunisia. Non si può dunque ritenere che abbia ancora raggiunto la forza di una legge consuetudinaria. Innanzitutto il suddetto trattato mira a garantire la protezione nel trattamento dei dati personali. Inoltre vieta il trattamento di dati riguardanti l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, quelli relativi alla salute o alla vita sessuale e su condanne penali. Viene garantito agli individui il diritto di conoscere i dati conservati su di essi. A tutto ciò viene posto come unico limite il contrasto con un interesse superiore quale possono essere sicurezza

[86] Convenzione n.108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale firmata a Strasburgo il 28 gennaio 1981. Entrata in vigore l'1 ottobre 1985 in seguito a cinque ratifiche. L'Italia dopo aver firmato la Convenzione 108 il 2 febbraio 1983, ha depositato gli strumenti di ratifica solamente il 29 marzo 1997, ed il trattato è così entrato in vigore l'1 luglio 1997. In data odierna, 21 settembre 2016 sono parte del trattato 50 stati.

nazionale o difesa dell'ordine. Sono infine limitati i flussi transfrontalieri di dati negli stati in cui il livello di protezione non sia adeguato.

2.4 L'Unione europea e la tutela dei dati personali

Dopo la sua fondazione anche l'UE ha posto al centro dei suoi impegni il rispetto dei diritti dell'uomo e dei valori sanciti dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali.

È in quest'ottica che un importante progresso nel campo della protezione dei dati personali è stato compiuto nel 1995 con l'adozione della direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati[87]. Questa direttiva mirava a uniformare le varie normative sulla protezione dei dati fra gli Stati membri, un requisito essenziale per garantire sicurezza alla libera circolazione dei dati all'interno dell'UE.

La direttiva trova la sua applicazione su dati trattati con mezzi automatici (come database informatici) e dati in archivi non automatizzati (come quelli cartacei)[88]. La direttiva non si applica invece alla manipolazione di dati a carattere prettamente domestico o personale, e a dati utilizzati per attività al di fuori dell'ambito di applicazione del diritto comunitario, come difesa e

[87] Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Entrata in vigore il 13 dicembre 1995, con obbligo di ricezione entro il 24 ottobre 1998. In Italia è stata ricevuta con Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali ed entrata in vigore nel maggio 1997. Abrogata in seguito all'entrata in vigore del d.lgs 196/2003

[88] Direttiva 95/46/CE articolo 3

pubblica sicurezza[89].

La direttiva stabilisce quali sono gli utilizzi per cui è lecito il trattamento dei dati e, in ogni caso, pone il consenso dell'individuo come requisito sempre necessario[90].

Inoltre il trasferimento di dati verso paesi terzi da un uno Stato membro viene autorizzato solo se il ricevente ha un livello di protezione adeguato[91].

All'articolo 28 prevede inoltre la formazione di un organismo di controllo indipendente per ciascuno Stato membro, che vigilasse a livello nazionale sulla protezione dei dati: questo portò alla nascita della autorità nazionali di protezione dei dati. Invece con all'articolo 29 veniva istituito il Gruppo di lavoro, formato da un rappresentante di ognuno di esse e da un rappresentante della commissione.

I suoi compiti sono elencati all'articolo 30 e sono principalmente quello di: (a) *esaminare ogni questione attinente all'applicazione delle norme nazionali di attuazione della presente direttiva per contribuire alla loro applicazione omogenea; (b) formulare, ad uso della Commissione, un parere sul livello di tutela nella Comunità e nei paesi terzi; (c) consigliare la Commissione in merito a ogni progetto di modifica della presente direttiva, ogni progetto di misure addizionali o specifiche da prendere ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali; (d) formulare un parere sui codici di condotta elaborati a livello comunitario.*

Inoltre il Gruppo di lavoro deve informare la Commissione nel caso in cui verifichi un'eccessiva divergenza tra le legislazioni di Stati membri. Può fornire indicazioni di propria iniziativa su questioni riguardanti la protezione dei dati personali. Infine redige una relazione annuale sulla situazione generale della tutela del trattamento dei dati personali all'interno della Comunità.

---

[89] Direttiva 95/46/CE articolo 13; Confr. Capitolo 5 sui PNR

[90] Direttiva 95/46/CE articolo 7

[91] direttiva 95/46/CE articolo 25; Confr. Capitolo 4 su Safe Harbour

Poiché gli effetti della direttiva erano rivolti esclusivamente agli Stati, nel 2001 venne formulato il Regolamento sulla protezione dei dati da parte delle istituzioni comunitarie(regolamento 45/2001/CE) in modo da estendere la protezione dei dati personali anche al trattamento effettuato da organismi ed istituzioni comunitari[92].
In particolare con questo Regolamento viene istituito il Garante europeo della protezione dei dati(GEDP), un'autorità di controllo che deve valutare l'applicazione di normative sulla protezione dei dati. Possono ricevere reclami dai cittadini, qualora questi ultimi ritengano che un loro diritto sia stato leso dal mancato rispetto del regolamento.

Una direttiva volta a regolare più nel dettaglio la vita privata e le comunicazioni elettroniche in modo più moderno è stata approvata nel 2002. La direttiva 2002/58/CE[93] in particolar modo regolava la conservazione dei dati sul traffico telefonico raccolti a fini di sorveglianza dalla polizia. Inoltre nel caso di brecce che portino alla violazione dei dati personali i fornitori hanno l'obbligo di inviare una notifica all'autorità nazionale garante e in taluni casi, a seconda della tipologia del dato compromesso, devono informare anche le persone interessate.

Un ulteriore grande traguardo raggiunto dall'UE è stato l'approvazione della Carta dei diritti fondamentali dell'Unione europea, detta Carta di Nizza,

[92] Regolamento 45/2001/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati. In vigore dal 1 febbraio 2001.
[93] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche). In Italia recepita all'interno del d.lgs 196/2003 Codice in materia di protezione dei dati personali, entrato in vigore il 1 gennaio 2004.

nel 2000[94]. Al suo interno viene collocata la tutela del diritto alla vita privata e familiare, infatti l'articolo 7 recita che *"ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".* Successivamente l'articolo 8 è riservato alla protezione dei dati personali e ciò viene dunque considerato un diritto fondamentale dell'individuo. Nel primo comma dell'Articolo viene dichiarato che "*ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano*". Il secondo specifica che "*tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica*". Infine il terzo comma enuncia che "*il rispetto di tali regole è soggetto al controllo di un'autorità indipendente*".

La divisione della tutela di questi diritti in due specifici articoli mostra l'evoluzione che si è verificata nei cinquant'anni successivi alla scrittura dell'articolo 8 della CEDU[95].

Entrato in vigore il Trattato di Lisbona il 1 dicembre 2009, la Carta di Nizza viene inclusa sotto forma di allegato e acquisisce così valore giuridicamente vincolante: in base all'articolo 6 del Trattato dell'Unione europea "*l'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adottata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati*".

[94] La Carta dei diritti fondamentali dell'Unione europea è stata proclamata a Nizza il 7 dicembre 2000, e una seconda volta nel dicembre 2007 a Strasburgo. Con l'entrata in vigore del "trattato di Lisbona" guadagna anch'essa valore giuridico vincolante di un trattato. La Gran Bretagna ha ottenuto un "opt-out" dalla Carta. Polonia e Repubblica Ceca hanno ottenuto, ma non esercitato un "opt-out"

[95] Pizzetti F.*, Il percorso del Consiglio d'Europa che porta al riconoscimento del diritto alla protezione dei dati personali*, LUISS, Consultabile su: http://docenti.luiss.it/privacy-pizzetti/tutela-e-protezione-dei-dati-personali-2/sintesi-lezione-6-ottobre-2010/

Infine nell'aprile 2016 è stato adottato il Regolamento UE 2016/679 del Parlamento europeo e del Consiglio[96], il regolamento generale sulla protezione dei dati (da qui in avanti RGPD o Regolamento), che entrerà in vigore a partire dal 2018 abrogando e mandando in pensione la Direttiva 95/46/CE, che sente ormai il peso degli anni visti gli esponenziali progressi tecnologici avvenuti dopo la sua istituzione e che quindi sempre più difficilmente si adattano al mondo odierno.

Innanzitutto il Regolamento ha il grande pregio di armonizzare le varie normative nazionali all'interno dell'Unione europea, che in passato, al momento di recepire la direttiva 95/46/CE hanno adottato scelte talvolta divergenti[97].

Il Regolamento è applicabile a tutti i dati che vengono trattati all'interno dell'Unione europea. Inoltre si applica anche a tutti i dati che vengono trattati da soggetti non europei, ma che trattino per l'offerta di beni e servizi dei dati di cittadini europei[98].

Sono implementati nel Regolamento gli obblighi di *privacy by design* e *privacy by default*. In altre parole, "*il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati di default*"[99].

Informare gli interessati e ottenere il loro consenso resta uno degli elementi fondamentali del Regolamento. Inoltre per particolari misure come la "profilazione" viene richiesta una valutazione d'impatto[100].

---

[96] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A32016R0679

[97] RGPD punto 3 dei 'considerando'

[98] RGPD punti 22 e 23 dei 'considerando' e articolo 27

[99] RGPD punto 78 dei 'considerando' e articolo 25

[100] RGPD punto 91 dei 'considerando' e articolo 13

Agli individui deve essere garantito un diritto di accesso e rettifica dei propri dati personali[101]. Sono inoltre creati dei nuovi importanti diritti quali "il diritto all'oblio"[102] e il diritto alla portabilità dei dati[103].

2.5 Il modello americano di protezione dei dati personali

Il modello americano di tutela della privacy e della protezione dei dati personali è completamente diverso da quello europeo, un aspetto che porta talvolta a contrasti nei rapporti transatlantici, come per esempio nella vicenda dei PNR o del Safe Harbour che analizzerò in seguito.

Se all'interno dell'Unione europea il tentativo è quello di una rigida regolamentazione che limiti allo stretto necessario la manipolazione dei dati personali, la situazione negli Stati Uniti è quasi opposta. La legislazione americana permette una maggiore invasione della privacy dei suoi cittadini, consentendo una più vasta raccolta di dati. Inoltre, a differenza dell'Unione europea, manca negli Stati Uniti un'autorità di controllo [104].

Un'altra grande differenza è il fatto che all'interno dell'Unione europea sia stata adottata una legge generale, prima la Direttiva 95/46/CE e a breve il Regolamento UE 2016/679, che regolamentano il trattamento dei dati personali in ogni suo possibile ambito e aspetto. Diversamente, negli Stati Uniti la scelta è stata quella di una legislazione frammentaria, creando un

[101] RGPD articolo 16
[102] RGPD articolo 17; confr. Capitolo 3
[103] RGPD articolo 20
[104] Marsha Cope Huie, Stephen F. Laribee, Stephen D. Hogan, 2002, *The right to privacy in personal data: the EU prods the US and controversy continues*, Tulsa Journal of Comparative and International Law, Vol. 9 Issue 2

sistema settoriale[105].

Senza dimenticare che gli Stati Uniti, un paese di *Common Law*, tutelano il diritto alla privacy in modo quasi esclusivamente giudiziario. È quindi fondamentale il ruolo della Corte Suprema degli Stati Uniti nell'evoluzione della giurisprudenza, la quale giudica in accordo alla Costituzione Federale[106]. In quest'ultima non vi è traccia di un esplicito riferimento al diritto alla riservatezza.

Vengono tuttavia anche promulgate delle leggi ad hoc che vanno a disciplinare alcuni specifici settori. Inoltre alcune di queste sono leggi federali. Una delle più importanti è costituita dal Freedom of Information Act (FOIA) emanata negli Stati Uniti il 4 luglio 1966. In base a quell'atto viene stabilito che chiunque ha diritto di accedere ai registri e agli archivi delle agenzie federali. Spetta al Governo l'onere di dare spiegazioni nel caso in cui la richiesta di accesso venga rifiutata. A tal riguardo, sono nove le eccezioni previste dall'atto e riguardano la protezione di interessi superiori, quali il rispetto della privacy o la sicurezza nazionale[107].

Dopo di ciò, nel 1974 il Congresso approvò il Privacy Act. Venne creato come conseguenza dello scandalo Watergate, nel quale si trovò invischiato e dovette dimettersi anche l'allora presidente Nixon. In quel momento era percepita l'assoluta necessità di porre dei limiti agli abusi che venivano commessi da agenzie ed enti pubblici nei confronti dei cittadini al riguardo di un uso improprio delle informazioni che li riguardano.
Nonostante i molti anni trascorsi dalla sua adozione rimane uno dei principali strumenti di protezione della privacy negli Stati Uniti.
Dal suo campo di applicazione rimangono però esclusi i soggetti privati, in

[105]Francesce Bignami, 2007, *European versus american liberty: a comparative privacy analysis of antiterrorism data mining*, Boston College Law Review Vol. 48:609
[106] Shaman, Jeffrey M., 2006, *The right of privacy in state constitutional law,* Rutgers Law Journal, Issue 4, Vol. 37, p. 971-1085
[107] Dipartimento di Giustizia degli Stati Uniti, *What is FOIA?* , consultabile su: https://www.foia.gov/about.html

quanto regola solamente il rapporto tra cittadini e organi del governo federale. Inoltre, il Privacy Act vale solo per il trattamento di dati appartenenti a cittadini statunitensi[108].

Altre leggi emanate a protezione della privacy con un ambito di applicazione molto limitato sono ad esempio la Tax Reform Act del 1976 che tutelava la privacy delle informazioni finanziarie, oppure la Driver's Privacy Protection Act del 1994 che impediva il rilascio di informazioni personali di un guidatore senza il suo consenso[109].

A parti casi isolati come i precedenti negli Stati Uniti vige un sistema della privacy settoriale in cui la protezione al cittadino viene garantita più con lo status di "consumatore". Vi sono principalmente due regolamentazioni possibili. Una, secondo i principi di "fair information practice", nella quale i punti fondamentali sono l'informativa per il consumatore, una richiesta di consenso, la possibilità di accedere e verificare i dati, garanzie di conservazione in sicurezza dei dati e misure atte a rispettare tali principi. Oppure con il sistema "permissible purpose" che limita il trattamento dei dati a finalità previste dalle leggi[110].

A quel punto è compito della Federal Trade Commission di vigilare sul rispetto delle imprese dei regolamenti da essi adottati e il controllo che non vi siano pratiche scorrette per i consumatori[111].

Il diritto alla privacy già scarsamente tutelato da questo approccio settoriale è stato ulteriormente compresso quando nel 2001 è stato approvato il Patriot Act[112], che ha ampliato notevolmente i poteri delle agenzie federali,

---

[108] Coles T.R., 1991, *Does the privacy act of 1974 protect your right to privacy?*, The american university law review, Vol.40:957

[109] R. LeRoy, F.B. Cross, 1996, *The legal environment today*, Miller Business Law

[110] P. Swire, S. Bermann, 2007, *Information privacy*, IAPP Publication

[111] M.P. Eisenhauer, 2008, *The IAPP Information Privacy Case Book*, IAPP Pubblication

[112] USA PATRIOT Act, acronimo di Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, legge federale statunitense fermata il 26 ottobre 2011 con l'obbiettivo di combattere il terrorismo. Ha ricevuto una proroga per alcune sue disposizioni nel 2005 ed un'ulteriore proroga di tre disposizioni nel 2011per 4 anni.

permettendo loro di accedere a informazioni personali ed effettuare intercettazioni.

Capitolo 3
La protezione dei dati personali e il "diritto all'oblio"

3.1 L'importanza di dimenticare: il concetto dell'"oblio"

Sul "diritto all'oblio" diversi autori si sono soffermati sull'importanza del fattore del tempo, analizzato sotto una duplice ottica: il tempo come marcatore del momento in cui dovrebbe cessare la conservazione dei dati e può far seguito l' "oblio", e il tempo come fattore che può aggiungere e togliere peso alle richieste di cancellazione dei dati personali.

Al riguardo del tempo Rosen aveva dichiarato in un articolo che "*il web significa la fine dell'oblio*"[113]. La memoria dell'uomo è imperfetta, consente di dimenticare quello che è stato, con la nascita del web invece è stata creata una ragnatela che non lascia più sfuggire nulla di ciò che cattura. Irrompe allora al centro del dibattito la necessità degli individui che certe cosa vengano dimenticate, che cadano nell' "oblio". Specialmente in quei casi in cui il tempo rende le informazioni caricate nel web decontestualizzate, superate o non più veritiere.

Si aprì subito un vivo dibattito, quando il RGPD era ancora una proposta e presentava al suo interno, per la prima volta, un diritto all'oblio, che all'articolo 17 viene descritto come "*il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza*

[113] Rosen, J. ,21 luglio 2010, *The web means the end of forgetting*, The New York Times, Consultabile su: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all

ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali".

Rosen aveva subito etichettato il diritto all'oblio come "*la più grande minaccia alla libertà di parola su internet della prossima decade*"[114].

Tuttavia, oltre a numerosi oppositori, il diritto all'oblio ha avuto ampio sostegno fra coloro che ritengono tale diritto come socialmente essenziale in un mondo che ha perso la capacità di dimenticare. Vi è anche chi ritiene che non essere capaci di dimenticare renda gli essere umani più restii a perdonare[115].

Viktor Mayer-Schönberger ricorda che nel XIX secolo Jeremy Bentham aveva ideato il panottico, un tipo di prigione in cui le guardie potevano osservare i detenuti senza che questi ultimi potessero saperlo. Nel XX secolo Michel Foucault argomentava che il modello del carcere panottico fosse usato in modo più astratto per esercitare un controllo sulla società. Le conclusioni a cui vuole giungere Mayer-Schönberger sono che ora, nel XXI secolo, il panottico si estende al cyberspazio, divenuto un luogo dove dobbiamo agire come se fossimo osservati, anche se non lo siamo. La perfetta memoria digitale può dunque avere l'effetto di renderci censori di noi stessi[116].

Mayer-Schönberger propone anche un mondo digitale dove ciò che viene caricato sulla rete abbia un data di scadenza, in modo da ridare valore alle cose. Che una foto ad esempio venga rimossa automaticamente dalla rete dopo un anno. E solo nel caso di eventi particolarmente importanti si possa selezione una data più lontana[117].

Il tempo è uno degli aspetti più interessanti della vicenda accaduta allo psicoterapeuta canadese, Andrew Feldmar. Nel 2006 si stava recando dalla

[114] Rosen, 2012, *The right to be forgotten*, Stanford law review online
[115] Mayer-Schönberger, nota 41
[116] idem
[117] idem

sua città di Vancouver all'aeroporto di Seattle e si accingeva dunque a oltrepassare la frontiera tra Canada e Stati Uniti, come era spesso solito fare. Tuttavia, in quell'occasione, l'agente di servizio alla dogana digitando il nome di Feldmar tra i risultati trovò un articolo che questi aveva scritto nel 2001 per una rivista scientifica, nel quale faceva cenno al fatto di aver fatto uso di LSD negli anni Sessanta. Dopo essere stato trattenuto per ore alla dogana, registrato le impronte digitali e firmato una dichiarazione di aver fatto uso della suddetta sostanza psicotropa, fu bandito dal suolo statunitense[118]. Andrew Feldman si ritrovò dunque a pagare le conseguenze di un reato commesso più di trent'anni prima. Un fatto che ormai era completamente alle sue spalle, che riguardava la persona che era un tempo e non quella che era diventata, uno scheletro che credeva di aver chiuso per sempre in un armadio, ma che in quel giorno si riaprì come nei peggiori incubi per via della perfetta memoria digitale. Un errore che in circostanze normali sarebbe stato già perdonato e dimenticato, ma nel momento in cui quella notizia viene letta per la prima volta su Internet, al lettore manca la percezione dell'intervallo di tempo che separa quel momento ad oggi e, benché risalga a moltissimo tempo addietro, non può perdonare l'accaduto.

La vicenda di Feldman dimostra dunque quanto una memoria perfetta come quella digitale sia pericolosa, e la necessità che sia possibile cancellare dalla rete notizie ormai datate.

Zittrain ironicamente propone che le persone possano dichiarare bancarotta per la loro reputazione ogni 10 anni, per avere una seconda o terza possibilità anche nel mondo digitale[119].

Nella maggior parte delle sentenze europee il diritto all'oblio è stato infatti solitamente adottato per proteggere gli individui da eventi del loro passato

[118] Mayer-Schönberger, nota 41

[119] Zittrain, 2008, *The Future of the Internet and How to Stop It*, Yale University Press & Penguin UK 2008, Consultabile su: https://dash.harvard.edu/bitstream/handle/1/4455262/Zittrain_Future%20of%20the%20Internet.pdf

che oggi li danneggiano in modo sproporzionato e ingiusto.

3.2 La nascita del “diritto all’oblio”: la sentenza Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González

Nel Regolamento generale sulla protezione dei dati del 27 aprile 2016 è presente l’articolo 17, un articolo riservato a trattare interamente il diritto alla cancellazione, detto anche “diritto all’oblio”. Come già anticipato questo articolo consente di ottenere una tempestiva cancellazione dei dati personali che riguardano una persona che ne faccia richiesta. Affinché possa valere l’articolo deve sussistere una delle seguenti condizioni: *(1) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; (2) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; (3) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; (4) i dati personali sono stati trattati illecitamente; (5) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; (6) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1*.

L’articolo 17 è opera di codificazione che va a cristallizzare una sentenza del 2014 della Corte di giustizia dell’Unione europea(CGUE). Si tratta del caso Google Spain SL, Google Inc. vs Agencia Española de Protección de

Datos, Mario Costeja González e la sentenza ha fatto la storia poiché aveva fornito una nuova interpretazione della Direttiva 95/46/CE per merito della quale viene per la prima volta riconosciuto ad un individuo il “diritto all’oblio”, ovvero per quanto concerne il web la possibilità di richiedere ad un motore di ricerca la rimozione dai risultati della ricerca dei link collegati al nome del richiedente, salvo alcune eccezioni.

La vicenda aveva avuto inizio quando un cittadino spagnolo cercando il proprio nome su Google aveva trovato fra i risultati della ricerca dei link che rimandavano a due pagine del quotidiano catalano “La Vanguardia" risalenti al 1998, nelle quali era presente l’annuncio della vendita all’asta della sua casa per questioni economiche. Il sig. González fece richiesta al quotidiano di rimuovere le pagine in cui figurava e a Google Spain e Google Inc. di nascondere dai risultati di ricerca le suddette pagine. Poiché la richiesta non venne accolta dalle parti decise allora di rivolgersi all’Agencia Española de Protección de Datos(in seguito AEPD), ovvero l’autorità di controllo spagnola che vigila sulla protezione dei dati personali, l’equivalente del Garante della Privacy italiano. L’AEPD fece cadere il reclamo nei confronti del quotidiano, in quanto la pubblicazione era a suo tempo legalmente giustificata. Accolse invece il reclamo nei confronti di Google Spain e Google Inc. e ordinò l’eliminazione dei dati. Google Spain e Google Inc. decisero di non ottemperare la richiesta in quanto vedevano in essa una limitazione della libertà di espressione. Le parti furono portate allora di fronte alla Corte di Giustizia dell’Unione Europea che doveva giudicare in primis se un motore di ricerca possa essere soggetto alle leggi europee, in secondo luogo se Google Spain debba rispondere del trattamento di dati che avviene in server situati negli Stati Uniti ed infine se un individuo abbia il diritto di chiedere che i

propri dati personali vengano rimossi dai risultati di una ricerca[120].

La Corte dopo aver esaminato la questione innanzitutto confermò in base all'articolo 2 della direttiva 95/46/CE, che l'attività di un motore di ricerca va qualificata come trattamento di dati personali e il gestore del motore di ricerca ne è responsabile e quindi soggetto a tale direttiva[121]. In quanto a Google Spain: sebbene i dati siano processati negli Stati Uniti da parte di Google Inc. il fatto che Google Spain sia una sua sussidiaria che promuove la vendita di spazio pubblicitario nel motore di ricerca, con sede in uno Stato membro, rende la legge europea applicabile. Stabilita l'applicabilità della Direttiva la Corte dichiarò che il diritto all'oblio è un diritto fondamentale dell'individuo che fa parte integrante del diritto al rispetto della vita privata e quindi pienamente garantito dall'articolo 8 della Carta di Nizza ed è dunque legittimo richiedere che informazioni personali vengano oscurate[122].

Questo vale ad eccezione del caso in cui ci sia un giustificato interesse pubblico ad accedere a quelle informazioni, poiché in quel caso prevarrebbe la libertà di espressione ed informazione. Infatti, per ironia della sorte, quando nel Marzo 2015 il Sig. González si rivolse nuovamente all'AEPD vide rifiutata la sua richiesta di ottenere la deindicizzazione da Google di alcuni articoli che trattavano la sentenza discussa in precedenza e che inoltre indagavano la sua vita personale, in quanto ritenute questa volta informazioni rilevanti per il pubblico e non obsolete[123]. A partire dalla sentenza della CGUE del 13 maggio 2014 discussa finora è stato dunque riconosciuto all'interno dell'UE il diritto all'oblio, senza avere però raggiunto al riguardo

[120] Sentenza della Corte (Grande Sezione) 13 maggio 2014, Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González, Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN

[121] Sentenza Google Spain, nota 120, punto 100

[122] Sentenza Google Spain, nota 120, punto 100

[123] Guido Scorza, 9 ottobre 2015, *Costeja Gonzalez: negato l'oblio all'uomo che lo ha regalato all'Europa*, Il fatto quotidiano, Consultabile su: http://www.ilfattoquotidiano.it/2015/10/09/costeja-gonzalez-negato-loblio-alluomo-che-lo-ha-regalato-alleuropa-2/2111057/

una chiara e precisa indicazione su come vada applicato.

3.3 L'estensione del "diritto all'oblio" globale

La situazione rimase controversa tant'è che l'anno successivo alla sentenza Google Spain ebbe inizio una nuova disputa al riguardo, stavolta fra Google e la Commission nationale de l'informatique et des libertés(CNIL), ovvero l'autorità di controllo francese in materia di protezione dei dati personali[124].

In seguito alla sentenza della CGUE, Google aveva iniziato a rimuovere dai risultati di ricerca le URL collegate a nomi di persone che ne avevano fatto richiesta. Tuttavia la rimozione veniva effettuata solamente nelle estensioni europee (ad esempio .it, .fr) del motore di ricerca lasciando però i link accessibili a chiunque usasse il motore di ricerca attraverso altre estensioni(ad esempio .com). Il Garante francese dunque riteneva che per rendere effettiva la sentenza della CGUE fosse necessario da parte di Google la rimozione dei link da tutte le estensioni del suo motore di ricerca. Google rifiutò di adeguarsi e il CNIL iniziò una procedura per sanzionare il motore di ricerca americano[125].

Prima dell'udienza Google propose una soluzione basata sulla geolocalizzazione: si rendeva disponibile a filtrare i risultati di ricerca in base alla posizione fisica della persona che eseguiva la ricerca. In altre parole qualora ad esempio avesse ricevuto la richiesta da un cittadino francese di

[124] Commission nationale de l'informatique et des libertés, 12 giugno 2015, *CNIL orders Google to apply delisting on all domain names of the search engine*, Consultabile su: https://www.cnil.fr/fr/node/15790
[125] CNIL, nota 124

rimuovere un link associato al suo nome, il suddetto link verrebbe oscurato da tutte le ricerche effettuate in Francia da qualunque estensioni del motore di ricerca(quindi sia quelle europee come .it e .fr che quelle non europee come .com)[126].

Secondo il CNIL la soluzione proposta da Google non garantiva però la piena protezione del diritto all'oblio: fuori dall'Europa il link sarebbe ancora stato accessibile a chiunque, all'interno dell'Europa(nell'esempio, Francia esclusa) il link sarebbe stato accessibile a chiunque usasse un'estensione non europea del motore di ricerca, e infine dalla Francia un utente avrebbe facilmente potuto aggirare la restrizione cambiando l'origine geografica del proprio indirizzo IP(ad esempio usando una Virtual Private Network, VPN)[127].

Il Comitato Ristretto del CNIL nella sentenza del 10 Marzo 2016 ha stabilito che il servizio del motore di ricerca Google rappresenta un singolo processo operativo e le differenti estensioni geografiche(.fr, .it, …) non possono rappresentare separati processi operativi[128]. Dunque conferma che per mettere in atto la sentenza della CGUE è necessaria la rimozione dei risultati da tutte le estensioni dei motori di ricerca. Inoltre il Comitato Ristretto del CNIL ha giustamente tenuto a ribadire nella sua sentenza che la decisione presa non va ad intaccare la libertà di espressione, poiché ciò che viene oscurato è solamente il link nei risultati dai risultati di una ricerca effettuata con il nome e cognome di una persona. Di fatto le pagine rimangono accessibili quando la ricerca viene eseguita con differenti termini. Infine Google ricevette una sanzione di 100.000 euro[129].

---

[126] Commission nationale de l'informatique et des libertés, 24 marzo 2016, *Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google*, Consultabile su: https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google

[127] idem

[128] Decisione del comitato ristretto del CNIL del 10 marzo 2016 n.2016-054 Consultabile su: https://www.cnil.fr/sites/default/files/atoms/files/d2016-054_penalty_google.pdf

[129] idem

Nel Giugno 2016 Google ha avviato una procedura di ricorso al Consiglio di Stato della Repubblica francese (Conseil d'État), il più alto tribunale nella giurisdizione amministrativa francese, per chiedere che venga annullata la decisione del CNIL[130].

Google sta cercando dunque di portare avanti la sua battaglia, dichiarando che il diritto all'oblio è una forma di censura che mette a rischio il diritto d'espressione. Inoltre ritiene che la richiesta del CNIL sia illegittima in quanto chiede di applicare globalmente un diritto europeo. A mio parere però il Conseil d'État non potrà che confermare la sentenza del CNIL, a maggior ragione ora che è stato approvato il RGPD e che il "diritto all'oblio" è stato inserito in un Regolamento europeo. Innanzitutto perché nell'attuare il diritto all'oblio nei confronti dei motori di ricerca va anche ricordato che, come ha voluto sottolineare il CNIL nella sua sentenza, le pagine web non vengono cancellate da internet, rimangono accessibili e l'unico effetto è quello di oscurarle dai risultati delle ricerche eseguite a partire dal nome e cognome dell'interessato. Quindi la libertà d'espressione è comunque preservata. Poi è bene ricordare che il diritto all'oblio non è un diritto assoluto: non consente di rimuovere indiscriminatamente qualunque link da internet che una persona non gradisca. L'articolo 17, paragrafo 3 specifica i limiti di questo diritto: *il diritto all'oblio non si applica qualora sia in contrasto con la libertà di espressione o con l'adempimento di un obbligo legale, o qualora il trattamento dei dati sia necessario per il pubblico interesse*.

Infine, è più che legittima la richiesta del CNIL che esso venga applicato globalmente a tutte le estensioni del motore di ricerca, poiché si tratta dell'unico modo per garantire l'applicazione di tale diritto. D'altronde credo che aggrapparsi al concetto di territorialità nel web sia fuorviante. Internet non

[130] Lucie Ronfaut, 19 maggio 2016, *Google affronte la Cnil devant le Conseil d'État sur le droit à l'oubli*, LeFigaro, Consultabile su http://www.lefigaro.fr/secteur/high-tech/2016/05/19/32001-20160519ARTFIG00142-google-affronte-la-cnil-devant-le-conseil-d-etat-sur-le-droit-a-l-oubli.php

ha davvero dei confini geografici, dovrebbe rappresentare più un'area neutra come lo spazio cosmico. E, come già detto in precedenza, è fin troppo facile aggirare eventuali restrizioni geografiche o far apparire altrove l'origine geografica della propria connessione. D'altronde applicare alcune regole sulla protezione dei dati dell'UE a livello globale non sarebbe molto diverso da quello che già avviene quando i motori di ricerca oscurano dai loro risultati i link a pagine che contrastano con la Digital Millennium Copyright Act (la legge statunitense sul copyright)[131]. In questo caso una legge statunitense viene applicata globalmente nel mondo virtuale di internet[132]. Bisogna tuttavia dare atto al fatto che i diritti sul copyright sono sicuramente un tema meno controverso, che ha raggiunto un grado di condivisione internazionale molto più elevato rispetto al diritto all'oblio che ha una storia molto più recente. Infatti la convenzione di Berna del 1886 può contare su 172 Stati parti[133]. Ciononostante non bisogna dimenticare che il diritto internazionale è proprio questo: un diritto flessibile, in continua evoluzione, fatto di consuetudini che nascono e che muoiono. Proprio per questo è assolutamente apprezzabile lo sforzo europeo nel definire maggiori regole che siano applicabili anche al web.

[131] Il Digital Millennium Copyright Act (DMCA) è una legge statunitense sul copyright approvata l'8 ottobre 1998. Per effetto di questa legge può capitare che alcuni risultati siano globalmente rimossi da Google, sostituiti dalla dicitura "*A seguito di una serie di reclami ricevuti ai sensi del Digital Millennium Copyright Act (Legge statunitense sul copyright), abbiamo rimosso x risultati da questa pagina. Se lo desideri, puoi leggere i reclami DMCA che hanno portato alla rimozione all'indirizzo LumenDatabase.org.*"

[132] G. Resta, V. Zeno-Zencovich, 2015, *Il diritto all'oblio su Internet dopo la sentenza Google Spain***,** Roma TrE-Press

[133] La Convenzione di Berna per la protezione delle opere letterarie e artistiche, adottata a Berna nel 1886. L'Italia ha aderito il 20 giugno 1978 con legge di ratifica n. 399

3.4 L'applicazione del "diritto all'oblio" nelle sentenze delle corti europee e dei Garanti nazionali della privacy

Il diritto all'oblio è molto recente e grazie alle sentenze diramate dalle varie Corti di Stati membri dell'UE, questo diritto viene di volta in volta definite in modo più chiaro e circoscritto.

La prima sentenza italiana sul tema del diritto all'oblio applicabile su internet è stata pronunciata il 3 Dicembre 2015 dal Tribunale di Roma[134].

Nel caso romano un avvocato aveva richiesto a Google la deindicizzazione di quattordici link che comparivano effettuando una ricerca con il suo nome e cognome. I link portavano ad articoli di cronaca riguardante vicende di illeciti da i quali non era però scaturita alcuna condanna. L'avvocato riteneva che questi articoli ledessero la sua immagine e per questo motivo ne chiedeva la cancellazione. Visto il fermo rifiuto di Google, questi si rivolse al Tribunale di Roma che però con la sua sentenza rigettò il ricorso. Nella motivazione vi è in parte un aspetto temporale: gli articoli in questione risalivano a due anni prima della richiesta di cancellazione. Trattandosi di fatti recenti il diritto all'oblio va bilanciato con il diretto di cronaca e il primo deve lasciare il posto al secondo. In secondo luogo il Tribunale ritenne il ruolo pubblico svolto dall'avvocato rende la questione di pubblico interesse facendo così prevalere il diritto di informazione al diritto all'oblio.

Possiamo poi confrontare la sentenza del Tribunale di Roma con quella del caso belga Oliver G. contro Le Soir, che ebbe esiti assai diversi[135].

Nel 2008 il quotidiano belga Le Soir aveva reso disponibili nei suoi archivi digitali alcuni vecchi articoli, tra cui uno risalente al 1994 riguardante il

[134] Tribunale di Roma, sez. I Civile, sentenza 24 novembre – 3 dicembre 2015, n. 23771
[135] Cour de cassation de Belgique, 29 aprile 2016, N° C.15.0052.F Le Soir contre Oliver G. Consultabile su: https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf

medico Oliver G. che, ubriaco al volante, aveva causato un incidente mortale. Dopo aver pagato il suo debito nei confronti della società il medico aveva chiesto nel 2010 al quotidiano di rendere anonimo l'articolo, ricevendo però un categorico rifiuto. Nel 2013 il Tribunale di prima istanza a cui le parti si erano rivolte obbligò il quotidiano Le Soir a sostituire il nome del medico con delle X. Il quotidiano si rivolse alla Corte d'Appello e la sentenza del 25 settembre 2014 definì un importante bilanciamento fra il diritto d'espressione e il diritto alla vita privata contenuti entrambi nella CEDU. Stabilì in primis che i fatti del 1994 non avessero valore di attualità, in secondo luogo che rendere anonimo il nome del medico non era di interesse pubblico in quanto si trattava di una figura non pubblica coinvolta in un incidente vent'anni prima e infine che pur rendendo anonime le versioni digitali, gli originali cartacei rimangono intatti e preservando l'integrità dell'articolo[136].

Le Soir si appellò infine all'ultimo grado giudiziario belga, la Cour de Cassation. Nella sua sentenza la Corte confrontò il diritto all'oblio garantito dall'Articolo 8 della CEDU con l'articolo 10 della stessa che garantisce la libertà di espressione. La Corte sentenziò che l'articolo online al riguardo di un evento temporalmente molto distante causava danni sproporzionati rispetto ai limitati benefici della libertà di espressione e di stampa[137].

In questo caso il diritto all'oblio dunque prevalse, e venne rinnovata la richiesta al quotidiano di rimuovere il nome del medico dagli articoli online. Dunque le uniche richieste lecite rivolte a Google, a un altro motore di ricerca o altri attori del web sono quelle che chiedono la rimozione di informazioni inadeguate, irrilevanti o non più rilevanti. Mai potrà essere chiesto di rimuovere contenuti rilevanti per l'interesse pubblico. Viene chiesto

[136] Hugh Tomlinson, 18 luglio 2016, *Case Law, Belgium: Olivier G v Le Soir. "Right to be forgotten" requires anonymisation of online newspaper archive***,** Inform's blog, Consultabile su: https://inforrm.wordpress.com/2016/07/19/case-law-belgium-olivier-g-v-le-soir-right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive-hugh-tomlinson-qc/
[137] idem

invece di preservare al diritto alla privacy e alla dignità degli individui.

Allo stato attuale è dunque lasciato molto al buon senso delle Corti europee valutare e stabilire quando prevalga il diritto all'oblio e quando invece prevalgano i diritti d'espressione e informazione: sono proprio queste sentenze che stanno aiutando a delineare e rendere meno astratto il diritto all'oblio. Se per esempio da una lettura dell'articolo 17 del RGPD è difficile stabilire quanto indietro si possa spingere un criterio temporale per poter ritenere un articolo non più rilevante ai fini dell'informazione, possiamo invece ricevere un'indicazione dalle sentenze in base alle quali un decennio potrebbe essere un giusto tempo.

Un punto critico non affrontato dell'articolo 17 è quello di una situazione paradossale che però si è effettivamente verificata nel Regno Unito nel 2015: nuovi articoli che raccontano il contenuto di link rimossi in base al diritto all'oblio. Quello che si era verificato è che una persona aveva richiesto a Google la rimozione di nove link di articoli che includevano dettagli di crimini minori. Poiché gli articoli erano datati e risalivano a una decina di anni prima, Google applicò correttamente il diritto all'oblio rimuovendo i link dai risultati di ricerca e dandone notifica al sito web proprietario. A quel punto il sito web pubblicò un nuovo articolo riguardante la rimozione dei link da parte di Google e inserendo al suo interno anche le storie di cronache che in quei link erano state raccontate. Il querelante chiese a Google anche la rimozione dei nuovi link in cui compariva il suo nome, ma il motore di ricerca si rifiutò in quanto trattavano notizie recenti e di interesse pubblico. Il querelante si rivolse allora all'Information Commissioner's Office(ICO, il garante della privacy inglese) per ottenere la rimozione dei link. L'ICO si pronunciò a favore del querelante, obbligando Google a rimuovere i link. Nella sua sentenza l'ICO riconosce che gli articoli riguardanti la deindicizzazione di link sono di interesse pubblico, tuttavia non è necessario che queste storie compaiano scrivendo il nome del querelante, poiché ciò avrebbe un impatto

negativo sulla privacy di quell'individuo, violandone i suoi diritti[138].

Per quanto riguarda il Garante della privacy italiano ha ben presto iniziato ad adottare i primi provvedimenti in risposta a segnalazioni di persone le cui richieste di deindicizzazione di pagine web con loro dati personali ritenuti obsoleti o di scarso interesse pubblico non erano state accolte da Google.

Nel 2014 il Garante ha valutato nove casi[139]. In sette di questi casi le richieste sono state respinte in quanto il Garante ha valutato corretta la decisione di Google di far prevalere l'interesse pubblico, poiché si trattava di casi molto recenti in cui vi erano addirittura ancora a disposizione dei gradi di giudizio.

Nei rimanenti due casi, il Garante ha invece accolto le richieste ricevute. In uno dei due casi, vi erano un gran numero di informazioni eccedenti che toccavano persone estranee ai fatti giudiziari raccontati nella pubblicazione[140].

Nel secondo caso l'articolo pubblicato danneggiava l'interessato, violando così la privacy, in quanto l'informazione dovrebbe limitarsi ai fatti essenziali alla vicenda e tralasciare le abitudini sessuali di una persona identificabile, come si è invece verificato nel caso in questione[141].

---

[138] Information Commissioner's Office, *Enforcement notice*, Consultabile su: https://ico.org.uk/media/action-weve-taken/enforcement-notices/1560072/google-inc-enforcement-notice-102015.pdf

[139] Garante della privacy, Newsletter n. 397 del 22 dicembre 2014 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623678#1

[140] Provvedimenti a seguito di richieste di cancellazione, dai risultati resi da un motore di ricerca, dei collegamenti alle pagine web che contengono il nominativo dell'interessato - 6 novembre 2014 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623877

[141] Provvedimenti a seguito di richieste di cancellazione, dai risultati resi da un motore di ricerca, dei collegamenti alle pagine web che contengono il nominativo dell'interessato - 11 dicembre 2014 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623978

3.5 Le linee guida del Gruppo di lavoro articolo 29

In aiuto alle corti per decidere come applicare il diritto all'oblio nelle varie cause sono state pubblicate delle Linee guida da parte del Gruppo di lavoro articolo 29[142].

Innanzitutto, il Gruppo di lavoro precisa che la rimozione potrà avvenire solo per risultati ottenuti dalla ricerca effettuato con il nome di un a specifica persona. L'informazione originale rimane accessibile se nella ricerca vengono adottati termini diversi o se si accede all'informazione attraverso un link diretto.

Per tutelare in modo adeguato i diritti degli interessati la deindicizzazione non deve limitarsi ai domini europei (come .fr, .it) ma va esteso a tutti i domini globali(come .com)[143].

Dalla richiesta di deindicizzazione vengono esclusi i motori di ricerca integrati in alcune siti, in quanto il loro operato è limitato alla raccolta di informazioni tratte da pagine specifiche. I loro risultati non possono comportare un danno rilevante all'individuo.

Viene poi sottolineato che un individuo potrà effettuare la richiesta di deindicizzazione dei suoi dati con qualunque mezzo. Inoltre non è necessario che questi contatti anche il gestore del sito. Una richiesta rifiutata dal motore di ricerca dovrà essere adeguatamente motivata, e l'interessato potrà comunque rivolgersi alle autorità garanti nazionali. Il garante dovrà anche verificare che vi sia un "chiaro collegamento" tra la persona che richiede la deindicizzazione e l'Unione europea.

Ai motori di ricerca non è posto un obbligo di avvertire il gestore del sito dell'avvenuta richiesta di deindicizzazione. Tuttavia, al fine di prendere una

[142] Linee guida nell'applicazione del giudizio della CGUE nel caso Google Spain Inc v. all'Agencia Española de Protección de Datos e Mario Costeja González C-131/12

[143] confr. Con nota 126, richiesta del Commission nationale de l'informatique et des libertés a Google

corretta decisione può essere talvolta utile contattare il sito per acquisire maggiori informazioni al riguardo.

I motori di ricerca nel caso che venga effettuata una ricerca attraverso nome e cognome dovrebbero sempre presentare una dicitura nella quale avvertono che alcuni risultati potrebbero essere stati rimossi. In questo modo si evita di far capire se una persona possa aver fatto richiesta di deindicizzazione di alcune sue informazioni[144].

Infine le linee guida forniscono dei criteri per guidare le autorità nazionali di fronte alle richieste di reclamo di persone alle quali il motore di ricerca ha rifiutato la richiesta di deindicizzazione. Per esempio deve essere valutata la figura del richiedente (ovvero se questi è o meno una figura pubblica), se l'interessato è minorenne, se l'informazione può arrecare dei pregiudizi al richiedente.[145]

3.6 La diffusione del "diritto all'oblio" al di fuori dei confini europei

Negli Stati Uniti il dibattito al riguardo è molto acceso. Secondo alcuni il diritto all'oblio contrasterebbe in modo insanabile con la Costituzione americana, in particolare con i principi del Primo Emendamento che garantiscono le libertà di parola e di stampa. In quest'ottica il diritto all'oblio sarebbe applicabile solo limitatamente a ciò è stato direttamente pubblicato dalla persona. La cosa più vicina al diritto all'oblio che è presente sul suolo americano è la California Senate Bill 568, la cosiddetta "Erase button

[144] Attualmente cercando un nome e cognome di Google compare la scritta "*Alcuni risultati possono essere stati rimossi nell'ambito della normativa europea sulla protezione dei dati*" e quindi questo aspetto delle Linee guida è stato effettivamente recepito

[145] Linee guida, nota 142

law"(legge del pulsante cancella) valida nello stato della California a partire dal 2015[146]. Questa legge tutela i minorenni su internet obbligando i siti web e le applicazioni mobile a cancellare su richiesta dei minori qualunque contenuto da loro pubblicato. Ha dunque degli effetti estremamente limitati, inoltre non garantisce alcuna protezione se a caricare dati personali sul minore sono dei terzi. Ciononostante la firma di questa legge provocò molto scalpore e la maggior parte dei critici ne vedeva un'incompatibilità con il Primo Emendamento[147]. Questo è stato finora il maggiore passo compiuto da uno stato federale americano verso una parziale garanzia della protezione dei dati degli utenti (minori). La distanza fra la visione europea e quella statunitense è dunque ancora molta. Quello che all'interno dell'Unione Europea è diventato un diritto pienamente riconosciuto, negli Stati Uniti rimane un principio di difficile applicazione che trova costantemente una ferrea resistenza da parte dei sostenitori di un'assoluta libertà di espressione, vista come un elemento fondante del loro Paese. Il piccolo progresso avvenuto in California potrebbe però essere la prima apertura che potrebbe poi diffondersi in altri Stati e aprire al cambiamento. D'altra parte diversi sondaggi svolti sul territorio statunitense hanno messo in risalto che la maggioranza dei cittadini statunitensi sarebbe favorevole a regolamentare il web con diritto all'oblio sul modello europeo. Non bisogna dimenticare che il diritto all'oblio è un diritto estremamente recente, la cui nascita viene spesso associata alla sentenza della CGUE del caso González-Google del 2014. Dunque un diritto nato appena due anni fa, inserito solamente quest'anno in un Regolamento europeo che sarà effettivamente applicabile dal 2018. È

[146] Kathleen Miles, 24 novembre 2013, *Teens Get Online 'Eraser Button' With New California Law, Huffington Post*, Consultabile su: http://www.huffingtonpost.com/2013/09/24/teens-online-eraser-button-california_n_3976808.html

[147] Gregory Ferenstein, 24 settembre 2013, *On California's bizzare Internet eraser law for teenagers*, Techcrunch, Consultabile su: https://techcrunch.com/2013/09/24/on-californias-bizarre-internet-eraser-law-for-teenagers/

ancora presto dunque per valutare quanto questo diritto possa estendersi al di là dei confini europei.

La sentenza del Conseil d'État sarà un importante tassello perché se non dovesse confermare la sentenza del CNIL renderebbe zoppo il "diritto all'oblio", rendendo la sua piena attuazione di fatto impossibile per quanto riguarda internet. Se invece, come ritengo probabile, confermerà la decisione presa dal CNIL nei confronti di Google, contribuirà a rafforzare questo neo-nato diritto. Sarà quello il momento in cui si giocherà la vera partita, perché a quel punto Google si troverà in un fuoco incrociato. Da una parte la legittima richiesta europea di rimuovere i link da qualsiasi estensione del motore di ricerca, e dall'altra i principi costituzionali statunitensi che danno maggiori garanzie alla libertà di espressione. Quali soluzioni? In un'ottica di vecchio stampo bisognerà forse iniziare a valutare caso per caso la localizzazione dell'autore dell'articolo di cui è richiesta la rimozione e in base a quello applicare i principi di quel territorio. Oppure giungerà finalmente il momento di raggiungere degli accordi che vadano oltre la visione territoriale, che per internet è totalmente inadeguata in quanto spazio senza reali confini, dove i dati possono transitare senza sforzo istantaneamente da un punto all'altro del pianeta.

Capitolo 4
Il trasferimento di dati personali verso Paesi terzi: dal safe harbour all' EU-US privacy shield

4.1 Il trasferimento di dati personali verso Paesi terzi

La Direttiva 95/46/CE entrata in vigore il 25 ottobre 1998 ha creato uno standard europeo della protezione dei dati personali molto elevato. Il Capo IV della direttiva tratta il trasferimento di dati personali verso paesi terzi (non appartenenti all'UE o allo Spazio Economico Europeo: Norvegia, Islanda, Liechtenstein) e in base all'articolo 25 paragrafo 1: "*Gli Stati membri dispongono che il trasferimento verso un paese terzo di dati personali oggetto di un trattamento o destinati a essere oggetto di un trattamento dopo il trasferimento può aver luogo soltanto se il paese terzo di cui trattasi garantisce un livello di protezione adeguato, fatte salve le misure nazionali di attuazione delle altre disposizioni della presente direttiva.*"

Il potere di stabilire se un paese fornisce un livello adeguato di protezione è assegnato alla Commissione, che può effettuare delle decisioni di adeguatezza, con il parere positivo del Gruppo ex Articolo 29 della Direttiva 95/46/CE. Il paragrafo 2 dell'articolo 25 specifica che "*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 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."

È anche rilevante notare che ai fini della valutazione del livello di protezione, ciò che deve essere valutato dalla Commissione non è soltanto la normative vigente in un determinato paese, bensì anche tutti i regolamenti e norme di sicurezze che vengono rispettate in modo non vincolante. Devono dunque essere valutate anche le cossidette "self regulation", cioè tutte quelle norme di comportamento che vengono adottate dalle varie aziende o da interi settori industriali.
A tal fine il Gruppo di lavoro ritiene che quando si valuta tale strumento non vadano analizzate tanto le dimensioni dell'impresa, bensì andare a verificare l'effettivo rispetto delle regole e la capacità di imporre eventuali sanzioni.
Inoltre se le self-regulation riguardano un intero settore, ciò costituisce un vantaggio in quanto a trasparenza, al contrario di un ambiente frammentario, che per il consumatore può costituire uno scenario confuso.
Un altro aspetto che va valutato attentamente è la possibilità di un trasferimento di dati ad aziende che non condividono gli stessi codici di regolamentazione. Dovrebbe essere invece proibito il trasferimento di dati a coloro che non offrono adeguate garanzie.
Nella valutazione è inoltre molto importante la trasparenza delle regole, che queste siano scritte in modo chiaro e senza possibili fraintendimenti, magari fornendo anche delle esemplificazioni.
Vanno infine valutare tre caratteristiche delle self-regulation secondo il Gruppo di lavoro per poterle definire adeguate.
La prima è il rispetto delle regole. Al tal riguardo la presenza di un sistema di sanzioni può rappresentare una discreta garanzia per le protezioni offerte dal codice.

La seconda è la presenza di un organo indipendente che controlli la conservazione dei dati e offra aiuto per potervi accedere.
L'ultima caratteristica che dovrebbe essere presente è quella di meccanismi di riparazione nel caso in cui le regole vengano infrante. Vi deve essere una compensazione per i danni subiti.

Successivamente, nell'articolo 26 della direttiva vengono specificati i casi in cui il trasferimento ad un paese che garantisce una adeguata tutela viene comunque consentito in deroga all'articolo 25 paragrafo 2. Tali condizioni sono che:

a) la persona interessata abbia manifestato il proprio consenso in maniera inequivocabile al trasferimento previsto, oppure
b) il trasferimento sia necessario per l'esecuzione di un contratto tra la persona interessata ed il responsabile del trattamento o per l'esecuzione di misure precontrattuali prese a richiesta di questa, oppure
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto, concluso o da concludere nell'interesse della persona interessata, tra il responsabile del trattamento e un terzo, oppure
d) il trasferimento sia necessario o prescritto dalla legge per la salvaguardia di un interesse pubblico rilevante, oppure per costatare, esercitare o difendere un diritto per via giudiziaria, oppure
e) il trasferimento sia necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure
f) il trasferimento avvenga a partire da un registro pubblico il quale, in forza di disposizioni legislative o regolamentari, sia predisposto per l'informazione del pubblico e sia aperto alla consultazione del pubblico o di chiunque possa dimostrare un interesse legittimo, nella misura in cui nel caso specifico siano rispettate le condizioni che la legge prevede per la consultazione.

Ad oggi la Commissione ha riconosciuto solamente ad 11 nazioni un adeguato livello di protezione: Andorra, Argentina, Canada, isole Faer oer, Guernsey, Israele, Isola di Man, Baliato di Jersey, Nuova Zelanda, Svizzera e Uruguay[148].

I casi più significativi sono probabilmente quelli dell'Argentina, del Canada e della Svizzera, i cui ordinamenti federali sono stati giudicati idonei secondo i parametri comunitari e in cui è stata trovata una sufficiente corrispondenza di tutela della privacy.

La Svizzera è stato il primo paese a ricevere una decisione di adeguatezza positiva, il 26 luglio 2000[149].
La decisione prendeva in esame il Swiss Federal Act on Data Protection (SFADP) e su di esso il gruppo di lavoro aveva espresso alcune preoccupazioni[150]. I limiti messi in luce dall'analisi del Gruppo di lavoro sono legate al trasferimento verso i paesi terzi per il quale mancano restrizioni, l'assenza di un obbligo di informare gli interessati riguardo al trattamento dei dati, mancanza di strumenti atti a risolvere le controversie.
Tuttavia grazie all'inserimento di alcune clausole per tutelare maggiormente i dati personali nelle Costituzioni della maggior parte dei cantoni, la Commissione ha deciso di valutare positivamente i progressi fatti per allinearsi agli standard europei.

Successivamente il Canada ha ricevuto una decisione di adeguatezza

[148] Decisione della commissione sul livello di adeguatezza della tutela dei dati personali dei paesi terzi, Consultabile su:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm
[149] 2000/518/CE: Decisione della Commissione, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE, Consultabile su:
http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32000D0518&from=EN
[150] Opinion No 5/99 on The level of protection of personal data in Switzerland, Consultabile su:
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp22_en.pdf

positiva, il 20 dicembre 2001[151].

La decisione valutava positivamente la legge sulla privacy canadese, "*Canadian Personal Information Protection and Electronic Documents Act*". Questa legge che tutela informazioni personali e documenti elettronici è entrata in vigore il 1 gennaio 2001 e tutela i dati personali conservati da enti, organizzazioni e imprese che operano a livello federale. Dal 2004 questa legge si applica a tutte le organizzazioni, a prescindere che siano federali o meno, purché raccolgano dati personali a fini commerciali. A livello provinciale possono essere possono essere adottate diverse norme dagli organi locali a patto che siano in linea con i principi della legge federale sulla privacy[152]. Nella sua opinione favorevole il Gruppo di lavoro avverte la necessità di uno stretto controllo delle normative provinciali ed in particolar modo di quelle applicate in Quebec[153].

Poi, il 30 giugno 2003 la Commissione ha valutato in modo positivo il livello di adeguatezza argentino nella tutela dei dati personali. Per quanto riguarda l'Argentina la valutazione è stata portata su norme che hanno carattere generale e altre settoriale[154].

Anche in questo caso il parere positivo è accompagnato dall'opinione favorevole del Gruppo di lavoro che tuttavia avverte, come nel caso canadese, della necessità di un controllo dell'effettiva applicazione delle

---

[151] 2002/2/CE: Decisione della Commissione, del 20 dicembre 2001, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)

[152] Commissione europea, *Frequently asked questions on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents Act,* Consultabile su: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm

[153] Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act, Consultabile su: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp39_en.pdf

[154] 2003/490/CE: Decisione della Commissione, del 30 giugno 2003, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina, Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32003D0490&from=EN

norme a livello provinciale[155].

Oltre a questi tre casi la Commissione ha emesso delle decisioni di adeguatezza sull'adeguata tutela dei dati personali di Guernsey il 21 novembre 2003, dell'Isola di Man il 28 aprile 2004, del Baliato di Jersey l'8 maggio 2008, delle isole Faer Oer il 5 marzo 2010, di Andorra il 19 ottobre 2010, di Israele il 31 gennaio 2011, dell'Uruguay il 21 agosto 2012, ed infine della Nuova Zelanda il 19 dicembre 2012.

4.2 L'accordo safe harbour

Il sistema statunitense sulla protezione dei dati era sviluppato in modo molto diverso da quello europeo e non si sarebbe qualificato come sistema in grado di garantire la sicurezza dei dati personali secondo gli standard comunitari. Per riuscire a superare l'impasse ed evitare una situazione che avrebbe avuto effetti molto negativi sugli scambi tra l'UE e gli Stati Uniti, il dipartimento del commercio statunitense mise appunto dei principi. Si trattava di uno strumento su base volontaria rivolto alle imprese ed organizzazione americane per adeguarsi al livello di protezione richiesto dalla Direttiva 95/46/CE ed essere così dichiarate "approdo sicuro" (in inglese il cosiddetto "Safe Harbour"), con annessa dichiarazione di "adeguatezza".

Il 26 luglio 2000 la Commissione approvò una decisione di adeguatezza offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti»

[155] Opinion 4/2002 on the level of protection of personal data in Argentina, Consultabile su: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2002/wp63_en.pdf

(FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

I principi del "Safe Harbour" erano costituiti da sette punti fondamentali: notifica, scelta, trasferimento successivo, sicurezza, integrità dei dati, accesso e garanzie di applicazione.

(1) Innanzitutto la notifica: le persone devono essere informate sulle finalità della raccolta dei dati che le riguarda, i modi per contattare l'organizzazione per avere ulteriori informazioni in merito o per effettuare reclami e all'eventuale utilizzo da parte di terzi[156].

(2) Il secondo punto è la scelta, ovvero la possibilità data alla persona di consentire o rifiutare che le informazioni personali siano rivelate a terzi, o che le informazioni siano utilizzate per fini diversi da quelli per cui erano stare raccolte in origine[157].

(3) Il terzo punto, ovvero quello del trasferimento successivo, entra in gioco qualora l'organizzazione abbia intenzione di trasferire i dati a terzi. Prima di farlo dovrà verificare che quest'ultimo aderisca anch'esso ai principi dell'approdo sicuro o che comunque risulti essere coperto da garanzie di adeguatezza agli standard richiesti[158].

(4) Il quarto punto riguarda la sicurezza: chi conserva dati personali deve prendere ogni possibile precauzione per evitare che quelle informazioni non vengano trafugate o che ve ne sia fatto un uso non conforme[159].

(5) Il quinto punto è l'integrità dei dati: le informazioni devono essere pertinenti allo scopo per il quale sono state raccolte[160].

---

[156] 2000/520/CE: Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti. Allegato 1. Dichiarata invalida il 6 Ottobre 2015 in seguito alla sentenza nella causa C-362/14 della Corte di giustizia dell'Unione europea.

[157] idem

[158] idem

[159] Decisione della Commissione, nota 156

[160] idem

(6) Il sesto punto è sull'accesso è stabilisce il diritto per gli individui di accedere alle informazioni personali raccolte su di essi da un'organizzazione e che possano correggerle o cancellarle se inesatte[161].
(7) Il settimo ed ultimo punto dei principi del Safe Harbour sono le garanzie di applicazione: devono essere previsti dei meccanismi che garantiscano che le regole vengano efficacemente attuate. Per esempio vi devono essere meccanismi di ricorso indipendenti che permettano di risolvere eventuali contenziosi sulla base dei principi istituiti. Vi devono essere procedure di controllo per verificare l'effettivo rispetto degli impresi presi dalle organizzazioni riguardo alla riservatezza dei dati personali raccolti. Vi deve essere l'obbligo di rimediare a problemi causati dalla mancata applicazione dei principi, e sanzioni sufficientemente pesanti da garantire il rispetto dell'applicazione dei principi[162].

4.3 La caducazione dell'accordo Safe Harbour

Il Safe Harbour ha consentito e regolato per più di 10 anni il trasferimento di dati personali dall'Europa ad aziende e organizzazioni americane. Sarà la battaglia contro Facebook di uno studente austriaco, Max Schrems, per la protezione dei propri dati personali a portare alla decadenza di questo accordo. I dati personali degli utenti europei vengono trasferiti dalla filiale irlandese di Facebook (sede europea di Facebook) ai server situati sul suolo americano, dove il diritto e la prassi americana non offrono una sicurezza adeguata contro la sorveglianza svolta da autorità pubbliche.

[161] idem
[162] idem

Nel 2011, Schrems aveva richiesto a Facebook di vedere i propri dati personali conservati sui server americani di Facebook. Da Facebook ricevette i suoi dati dei tre anni precedenti, a partire dall'iscrizione sul sito, tra i quali erano compresi anche dati da lui cancellati ma che venivano invece ancora trattati da Facebook. Preso atto della scarsa tutela della privacy garantita da Facebook, Schrems denunciò varie volte quest'ultimo al Data Protection Commissioner, l'Autorità garante della privacy irlandese, richiedendo un blocco al trasferimento dei dati dalla filiale irlandese ai server americani. Nel 2012 a seguito di un'indagine l'Autorità irlandese predispone delle raccomandazioni a Facebook di adeguarsi alla normativa europea e garantire la cancellazione definitiva dei dati qualora richiesto[163].

Nel 2013 le rivelazioni di Edward Snowden misero in luce la sorveglianza di massa effettuata dalle agenzie di intelligence americane (in modo particolare da parte della National Security Agency, NSA) a scapito di tutti i dati presenti sul suolo americano, a prescindere dalla loro provenienza. In seguito alle rivelazioni, Schrems si rivolse nuovamente all'Autorità irlandese denunciando la scarsa sicurezza dei dati trasferiti nei server americani di Facebook. La denuncia venne però respinta dall'Autorità irlandese rimandando alla decisione della Commissione del 26 luglio 2000 in base alla quale il regime di "approdo sicuro" degli Stati Uniti venivano dichiarato avere un livello adeguato di protezione dei dati personali trasferiti. Successivamente, Schrems fece ricorso alla High Court of Ireland (Alta Corte di giustizia irlandese), la quale per poter valutare la questione si rivolge a sua volta, mediante rinvio pregiudiziale, alla Corte di Giustizia Europea[164]. Alla Corte viene chiesto se la decisione della Commissione del 26 luglio 2000 abbia tra i suoi effetti quello di impedire ad un'autorità nazionale di controllo di poter

[163] Europe-v-facebook, http://www.europe-v-facebook.org/CJEU_IR.pdf
[164] Sentenza Schrems vs Data Protection Commissioner della High Court of Ireland del 18 Giugno 2014

aprire un'indagine in seguito ad una denuncia contro un paese terzo che dia motivo di preoccupazione in quanto ad una non adeguata protezione dei dati personali, e se sia tra i suoi poteri quello di sospendere il trasferimento di dati in oggetto.

La Corte nella sua sentenza del 6 ottobre 2015 reputò che l'esistenza di una decisione della Commissione che dichiara che un paese terzo garantisce un livello di protezione adeguato dei dati personali trasferiti non può sopprimere e neppure ridurre i poteri di cui dispongono le autorità nazionali di controllo in forza della Carta dei diritti fondamentali dell'Unione europea e della direttiva[165]. Infatti la Direttiva 95/46 dà alle autorità nazionali i poteri di valutare se il trasferimento dei dati di una persona verso un paese terzo rispetta i requisiti comunitari sulla protezione dei dati, anche qualora vi sia una decisione della Commissione che dichiara adeguato il livello di sicurezza di quel paese. La Corte passando poi a valutare la validità della decisione della Commissione dichiara che quest'ultima si è limitata ad esaminare il regime dell'approdo sicuro senza prendere in considerazione anche altri aspetti come la legislazione nazionale o gli impegni assunti in campo internazionale[166]. La Corte rilevò che il regime di approdo sicuro è applicabile alle imprese americane ma non alle autorità pubbliche, che non sono tenute alla sua osservanza. Inoltre osserva che al regime dell'approdo sicuro prevalgono le esigenze di sicurezza nazionale e della legislazione americana, obbligando le imprese americane a disapplicare senza alcun limite le norme dell'approdo sicuro qualora siano in contrasto con tali esigenze[167]. Sono dunque possibili ingerenze da parte delle autorità pubbliche americane che

[165] Sentenza della Corte di giustizia nella causa Maximillian Schrems contro Data Protection Commissioner (Schrems), C-362/14, ECLI:EU: C:2015:650 del 6 ottobre 2015, punto 66
[166] Schrems, nota 165, punto 78
[167] Schrems, nota 165, punti 79-98. Per esempio in base all'articolo 702 della legge relativa alla vigilanza sull'intelligence esterna (FISA) ai servizi della comunità dell'intelligence statunitense viene consentito di poter richiedere l'accesso a informazioni, tra le quali anche i contenuti delle comunicazioni via Internet, che, sebbene siano conservate all'interno degli Stati Uniti, riguardano tuttavia cittadini stranieri che sono situati al di fuori degli USA.

possono accedere in maniera generalizzata ai dati personali delle persone ledendo così al diritto fondamentale del rispetto della vita privata. Infine, la Corte giunge a invalidare la decisione della Commissione del 26 luglio 2000, fino a quel momento adottato da oltre 4500 imprese americane per trattare i dati di cittadini europei[168].

4.4 L'accordo EU-US privacy shield, lo scudo della privacy

In seguito all'annullamento dell'accordo gli stati membri hanno concesso un breve periodo di grazia per consentire di attuare delle contromisure. Il Garante italiano Soro a inizio Gennaio 2016 parlava di "rischi di pesanti conseguenze dal punto di vista economico" nel caso in cui non si fosse giunti rapidamente ad un nuovo accordo che rimpiazzasse il regime di approdo sicuro[169].

Così il 2 febbraio 2016 la Commissione europea raggiunge un accordo su un nuovo regime che regoli gli scambi transatlantici di dati personali a fini commerciali con il governo degli Stati Uniti[170]. Il nuovo accordo ha preso il nome di "scudo UE-USA per la privacy" ed è stato adottato il 12 luglio 2016[171].

L'accordo si presenta come una forma rivisitata del "Safe Harbour" che richiede alle aziende americane maggiori controlli ed offre maggiori garanzie ai cittadini europei.

---

[168] Schrems, nota 165, punto 106

[169] Lettera del Presidente del Garante privacy, Antonello Soro, al Presidente del Consiglio dei Ministri, Matteo Renzi del 21 gennaio 2016

[170] Comunicato stampa della Commissione Europea del 2 febbraio 2016, Consultabile su http://europa.eu/rapid/press-release_IP-16-216_it.htm Accesso: 10 Settembre 2016

[171] Pubblicato nella Gazzatta Ufficiale dell'Unione Europea con decisione di esecuzione (UE) 2016/1250 della Commissione del 12 luglio 2016 a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy

I principi su cui si basa sono i seguenti: in primis, degli obblighi rigorosi per le imprese che trattano dati personali di cittadini europei. Al Dipartimento del Commercio degli Stati Uniti sono assegnati maggiori poteri e tra di essi vi è quello di sottoporre le imprese a verifiche e aggiornamenti periodici per controllare il rispetto dei diritti individuali. Lo stesso livello di protezione deve essere garantito anche quando avviene un trasferimento successivo a terze parti.

Il secondo punto riguarda gli obblighi di trasparenza per l'accesso da parte del governo degli Stati Uniti: gli Stati Uniti hanno offerto una garanzia scritta all'UE che l'accesso delle autorità pubbliche sarà soggetto a limitazioni ed eccezione a ciò saranno preso solo nella misura necessaria e in modo proporzionato. Viene inoltre aggiunto un meccanismo di ricorso all'interno del Dipartimento di Stato accessibile a qualunque cittadino dell'UE: un meccanismo di mediazione.

Il terzo punto riguarda la tutela effettiva dei diritti che viene garantita con la creazione di meccanismi di risoluzione delle controversie. Le imprese devono rispondere entro tempi precisi alle denunce. Le persone potranno anche rivolgersi presso le autorità nazionali di protezione dei dati, che potranno portare le loro denunce di fronte al Dipartimento del commercio e la Federal Trade Commission. Nel caso in cui non venga trovata una soluzione è possibile come *extrema ratio* sottoporre il caso ad arbitrato. L'ultimo punto riguarda un'analisi annuale comune, ovvero un'analisi congiunta della Commissione europea e del Dipartimento del Commercio degli Stati Uniti in modo da controllare il corretto funzionamento dello scudo, combattere la criminalità e garantire la sicurezza nazionale[172].

Ad aprile la bozza della proposta di accordo Privacy Shield presentata dalla Commissione era stata accolta positivamente dal Gruppo di lavoro ex

[172] Comunicato stampa della Commissione europea del 12 Luglio 2016, Consultabile su: http://europa.eu/rapid/press-release_IP-16-2461_it.htm Accesso: 10 Settembre 2016

Articolo 29, il quale riconosceva agli Stati Uniti i progressi fatti nei precedenti cinque mesi per adeguarsi alle richieste europee, in particolare elogia la maggior trasparenza offerta da parte statunitense. Il Gruppo di lavoro valutava positivamente l'introduzione di un meccanismo indipendente di controllo e il fatto e la possibilità dei cittadini europei di accedere a strumenti giudiziari.[173]

A maggio invece il Garante europeo della protezione dei dati emise il suo parere sull'accordo e non fu altrettanto positivo, ritenendo necessari numerosi miglioramenti.
In particolare il Garante si sofferma sui nuovi requisiti che verranno richiesti dall' articolo 45 del regolamento generale sulla protezione dei dati dell'UE. Per la valutazione dell'adeguatezza va anche tenuto conto che la soglia affermata dalla Corte di giustizia europea nella sentenza "Schrems" è quella della "sostanziale equivalenza"[174]. Gli Stati Uniti dovrebbero dunque garantire tutti gli elementi chiave previsti in materia di protezione dei dati europea. Il Garante ritiene dunque probabile un'ulteriore invalidazione dell'accordo da parte della CGUE, e critica la scarsa lungimiranza dell'accordo, che potrebbe portare presto ad una nuova situazione di incertezza per le imprese.
Un ulteriore critica del Garante è rivolta alla necessità di controlli più mirati nelle operazioni di *signal intelligence*[175], con le quali una quantità molto elevata di dati potrebbe essere oggetto di raccolta e uso.
In conclusione il Garante dichiara che lo scudo della privacy può essere un passo nella giusta decisione ma richiede ancora miglioramenti che lo portino a tutelare maggiormente i diritti dell'individuo alla vita privata e alla protezione

[173] Parere 01/2016 WP238 sulla decisione di adeguatezza della bozza di accordo "Privacy Shield EU-US", Consultabile su: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf
[174] Schrems, nota 165, punti 71, 73, 74 e 96
[175] attività d'intelligence attraverso captazione di segnali

dei dati personali previsti dall'UE suggerendo l'adozione di regole più specifiche per regolare l'accesso alle autorità americane ai dati personali e la necessità di adeguare l'accordo ai principi di "privacy by design" e "privacy by default", previsti dal nuovo Regolamento sulla protezione dei dati. [176]

[176] Sintesi del parere del Garante europeo della protezione dei dati sul progetto di decisione in merito all'adeguatezza dello scudo UE–USA per la privacy

Capitolo 5
La battaglia europea sui PNR e la sua evoluzione normativa

5.1 La sicurezza aerea negli Stati Uniti

Innanzitutto, i dati dei passeggeri vengono raccolti dalle compagnie aeree per motivi commerciali. Per esempio la prenotazione del volo, l'aeroporto di origine e di destinazione, eventuali richieste particolari del passeggero e la sua eventuale partecipazione al programma Frequent Flyer. Queste informazioni vengono conservate dalla compagnia aerea[177].

Oltre alla compagnia aerea anche lo Stato è interessato ad avere accesso a quei dati raccolti ai fini del controllo dell'immigrazione e per la sicurezza pubblica.

I meccanismi di sorveglianza iniziali erano alquanto limitati: nel 1944 l'Articolo 29 della Convenzione di Chicago richiedeva ad ogni vettore aereo in tratte internazionali il possesso di alcuni documenti, e riguardo ai passeggeri, una lista dei loro nomi e le indicazioni dei punti di partenza e di destinazione[178].

L'introduzione di maggiori regole e controlli fu la conseguenza di atti di terrorismo compiuti su voli aerei, di cui il primo si verificò nel 1968 con un

[177] Olga Mironenko, 2010, *Air Passenger Lists in Civil Aviation*, Kapittel 11

[178] Convenzione sull'aviazione civile internazionale, nota come Convenzione di Chicago, fu firmata a Chicago il 7 dicembre 1944. È entrata in vigore il 4 aprile 1947 in seguito alla 26ª ratifica. Ad oggi, gli stati membri del trattato sono 191, compresa l'Italia per la quale la Convenzione è in vigore dall'8 giugno 1948.

dirottamento ad Algeri del volo Roma – Tel Aviv della compagnia israeliana El Al.

Sulla fine degli anni ’90 furono cominciati ad essere sviluppati dei programmi di database incrociati. Il primo programma di sicurezza, nominato Computer Assisted Passenger Prescreening System (in seguito CAPPS) fu introdotto negli Stati Uniti dall’amministrazione Clinton nel 1999, in reazione alla misteriosa esplosione del volo TWA 800. Questo sistema prevedeva la creazione di un database di individui noti o sospetti di costituire una minaccia, e qualora uno di costoro si fosse imbarcato in un viaggio sarebbe stato sottoposto a controlli più rigidi[179].

In seguito agli attentati alle torri Gemelle di New York del 11 settembre 2001, le misure di sicurezza furono ulteriormente ampliate. Poche settimane dopo gli attentati entrò in vigore l’obbligo per i vettori aerei di rendere disponibili i Passenger Name Records(in seguito PNR) presenti nei loro archivi elettronici[180].

I PNR contengono, qualora disponibili, le seguenti informazioni:
(1) codice PNR della registrazione, (2) la data di prenotazione o emissione dei biglietti, (3) le date previste del viaggio, (4) Nome e cognome del passeggero, (5) informazioni sull’eventuale partecipazione al programma Frequent Flyer o altri benefici, (6) nomi e numero delle persone segnati sul PNR e ,(7) tutte le informazioni sui contatti di emergenza disponibili, (8) tutti i dettagli di pagamento(ad esempio, informazioni sulla carta di credito), (9) l’itinerario di viaggio specifico del PNR, (10) agenzia di viaggio, (11 informazioni sui codici condivisi con altri vettori, (12)) informazioni separate (quando un PNR contiene riferimenti ad un altro PNR, (13) status del

[179] David H. Holtzman, 2006, *Privacy Lost: How Technology Is Endangering Your Privacy*, Jossey-Bass

[180] In base all’ US Aviation and Transportation Security Act del 19 novembre 2001, tutte le compagnie aeree che partono o raggiungono gli Stati Uniti devono consegnare al US Bureau of Customs and Border Protection (CBP) e alla Transportation Security Agency (TSA) i dati personali contenuti nei PNR dei passeggeri. Tutte le agenzie federali statunitensi possono accedervi.

passeggero (ad esempio conferma del check-in), (14) informazioni generali sui biglietti,(15) informazioni sui bagagli, (16) numero di posto assegnato, (17) altre informazioni varie quali ad esempio la richiesta di servizi speciali o supplementari, (18) tutte le informazioni richieste dal sistema API[181], cioè nome, sesso, data di nascita, nazionalità, indirizzo di residenza, tipo di documento di viaggio(normalmente il passaporto), numero del documento di viaggio(oltre alla data di scadenza e paese di emissione), (19) tutta la cronologia di modifiche apportate ai punti precedenti.[182]

Queste informazioni restano conservate nei database della US Homeland Security per un periodo normalmente non superiore ai 15 anni. Dopo i primi sei mesi vengono resi anonimi mascherando alcuni elementi come nome, indirizzo e contatti, e qualsiasi aspetto possa direttamente identificare il passeggero. Per i primi cinque anni sono liberamente accessibili da tutte le agenzie federali, poi per i successivi dieci anni sono mantenuti in uno stato dormiente, durante il quale per accedervi un agente deve ottenere un'approvazione, che è concessa nei casi in cui una minaccia identificabile[183].

Come si può notare la quantità di informazioni a cui possono accedere le autorità americane è notevole, e molte si esse sono "informazioni sensibili". Inoltre, un PNR viene creato ogni qualvolta una persona effettua una prenotazione, e non può essere cancellato: una volta creato, viene infatti subito inserito in un database, *computer reservation system*(CRS), e può essere visualizzato anche qualora alla fine la persona non acquisti il biglietto o cancelli la prenotazione. Le agenzie di viaggio usano solitamente database del CRS per tutti i loro clienti. Vengono dunque salvate le informazioni anche

[181] APIs Advanced passenger information system (sistema avanzato sulle informazioni dei passeggeri)

[182] U.S. Department of Homeland Security, U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, Consultabile su: https://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf

[183] idem

di persone che non hanno mai viaggiato in aereo nella loro vita, ma che possono avere effettuato una prenotazione per un hotel o per il noleggio di un auto[184].

Il passo successivo negli Stati Uniti fu ridisegnare ed espandere il CAPPS nel CAPPS II nel 2003. Il CAPPS II come il suo predecessore utilizzava i dati raccolti dai PNR per effettuare un confronto con i database governativi degli elenchi “no fly” e “watch” per individuare eventuali passeggeri che avrebbero potuto rappresentare un rischio. In base a questo sistema ad ogni passeggero viene associato un punteggio di rischio e un codice di colore. La maggior parte dei passeggeri riceverà il “verde”, cioè nessun rischio e dovranno passare le procedure di controllo standard. In media l’8% riceve il “giallo”, che comporta maggiori controlli. Infine all’1-2% sarà associato il codice “rosso”. A questi sarà proibito l’imbarco e saranno sottoposti ad un interrogatorio o ad una perquisizione da parte della polizia e infine potrebbero anche essere arrestati[185].

Nel 2004 il CAPPS II venne rapidamente soppiantato in favore di un programma denominato *Secure Flight*, prodotto dell'"Intelligence Reform and Terrorism Act of 2004". Iniziati i test del programma nel 2005, questo subì un arresto nel 2006 per via dei numerosi casi di risultati “falsi positivi” e per le numerose critiche riguardo ad un’eccessiva invasione della privacy[186]. Il programma fu fatto ripartire qualche anno dopo, diventando operativo a partire dal 2009 per i voli domestici e dal 2010 per quelli internazionali.
Con il *Secure Flight* viene messo nelle mani del Dipartimento di Homeland Security(DHS) il compito di effettuare i confronti prima del volo tra le informazioni sui passeggeri e le liste di rischio dei governi federali.

[184] Edward Hasbrouck, *What's in a Passenger Name Record (PNR)?* Consultabile su: http://hasbrouck.org/articles/PNR.html
[185] Holtzman, nota 179
[186] Timothy M. Ravich, 2007, *Is Airline Passenger Profiling Necessary?,* 62 U. Miami L. Rev. 1

5.2 Il conflitto con tra Stati Uniti ed UE sui codici PNR

In seguito al *US Aviation and Transportation Security Act* del 19 novembre 2001, tutte le compagnie aeree che in partenza o in arrivo negli Stati Uniti devono preventivamente inviare alle autorità doganali statunitensi i dati personali contenuti nei PNR dei passeggeri e dell'equipaggio[187].

In questo modo la Transportation Security Agency (TSA), può confrontare questi dati con i registri governativi degli individui ad alto tasso di rischio e interdire a persone che risultano pericolose l'accesso al velivolo.

Esistono due metodi di trasmissione dei dati, uno è denominato "push" e l'altro "pull". Con il metodo "push" sono le compagnie aeree ad inviare i dati richiesti nei database delle autorità che li richiedono. Con il metodo "pull" invece le autorità che richiedono i dati ricevono dai vettori aerei libero accesso ai loro archivi e dunque possono direttamente prelevare una copia delle informazioni sui passeggeri.

A questo punto le compagnie aeree europee si ritrovarono sotto un fuoco incrociato. Da una parte la richiesta delle autorità americane di fornire i dati personali dei propri passeggeri, laddove una mancata soddisfazione delle richieste avrebbe potuto portare anche ad un divieto di atterraggio nel suolo statunitense per quelle compagnie. Dall'altra parte vi era la legislazione dell'Unione europea che vietava categoricamente quel trasferimento. I dati di persone fisiche raccolti per scopi commerciali ricadevano nell'ambito della Direttiva 95/46/CE e questa vietava il trasferimento di dati verso paesi terzi che non garantiscono un adeguato livello di protezione.

Già a giugno 2002 la Commissione europea avvertita le autorità statunitensi che vi era un conflitto con la legislazione europea sulla

[187] Mironenko, nota 177

protezione dei dati[188], pur comprendendo i legittimi interessi di sicurezza da cui la richiesta di accesso ai PNR scaturiva[189].

Gli Stati Uniti presero atto di ciò e decisero di posporre l'entrata in vigore delle nuove norme fino al 5 marzo 2003. Da quella data in poi avrebbero cominciato a sanzionare le compagnie aeree che non si fossero conformate al *US Aviation and Transportation Security Act* e a partire da allora molte grandi compagnie aeree europee hanno cominciato a dare accesso alle autorità statunitensi ai lori dati PNR[190].

Il 18 febbraio 2003, di fronte alla risolutezza americana, la Commissione decise di rilasciare una dichiarazione comune con l'amministrazione statunitense, con la quale venivano definiti i requisiti iniziali per la tutela dei dati operati dalle dogane statunitensi, e un accordo a continuare dei negoziati per far sì che le modalità d'uso dei PNR da parte delle agenzie statunitensi si avvicinassero alla normativa europea, in modo da soddisfare i requisiti dell'articolo 25, paragrafo 6, della direttiva 95/45/CE riguardo all'adeguata protezione dei dati trasmessi[191].

Nel giugno 2003 il Gruppo di lavoro "Articolo 29", istituito dalla direttiva 95/45/CE con compiti di tutela delle persone per quanto riguarda il trattamento dei dati personali, emanò un parere negativo, nel quale non giudicava essere sufficienti le garanzie degli Stati Uniti per il trasferimento di

[188] facevano riferimento in particolar modo (1) alla Direttiva 95/46/CE del Parlamento Europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e (2) al regolamento (CEE) N. 2299/89 del consiglio del 24 luglio 1989 relativo ad un codice di comportamento in materia di sistemi telematici di prenotazione

[189] Bart Van Vooren,Ramses A. Wessel, 2014, *EU External Relations Law: Text, Cases and Materials,* Cambridge University Law

[190] idem

[191] Comunicazione della Commissione al Consiglio e al Parlamento europeo - Trasferimento di dati di identificazione delle pratiche (PNR): un approccio globale dell'UE Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52003DC0826

dati PNR alle autorità di frontiera[192].

Prima di tutto il parere del Gruppo di lavoro valutava essere eccessiva la quantità di dati da trasmettere rispetto a quello che potrebbe essere ritenuto adeguato e pertinente, in base all'articolo 6, paragrafo 1, lettera c della direttiva 95/45/CE. Ritengono dunque che l'invio dei dati andrebbe limitato solo ad alcuni punti del PNR e non a questo nella sua interezza. In particolare dovrebbero essere esclusi dall'invio i dati di natura delicata, tutelati dall'articolo 8 della direttiva. In aggiunta a ciò il trasferimento non è considerabile come compatibile con il fine originario della raccolta.
Inoltre il periodo di 7-8 anni per il quale i dati verrebbero conservati è ritenuto troppo lungo. Secondo il gruppo di lavoro i dati andrebbero rimossi dagli archivi dopo alcune settimane, mesi al massimo[193].
Riguardo al trasferimento di dati l'unico che rispetta la direttiva è il sistema "push" in cui sono le compagnie aeree a fornire alle autorità americane i dati di cui hanno bisogno[194].
Sono poi considerate poco chiare le modalità di utilizzo dei dati: questi dovrebbero essere utilizzati per la lotta contro atti di terrorismo, mentre non dovrebbero essere estesi ad altri reati gravi[195].

Successivamente, il 29 gennaio 2004 il Gruppo ex. Articolo 29 ribadì il suo parere negativo e la presenza di punti di criticità nel trasferimento di PNR negli Stati Uniti[196]. Il nuovo parere faceva seguito ad una dichiarazione di

[192] Parere 4/2003 sul livello di protezione assicurato negli Stati Uniti per quanto riguarda la trasmissione di dati relativi ai passeggeri del 13 giugno 2003 - WP 78 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1609396
[193] Parere 4/2003, nota 192, punto 7 "Proporzionalità"
[194] Parere 4/2003, nota 192, punto 5 "metodo di trasmissione e problemi giuridici"
[195] Parere 4/2003, nota 192, punto 6 "scopi"
[196] Parere 2/2004 sul livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche Passeggeri (PNR –Passenger Name Record) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (Bureau of Customs and Border Protection - US CBP) del 29 gennaio 2004 - WP 8 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1608542

impegni statunitense[197] e una comunicazione della Commissione europea che presentava l'intenzione di raggiungere un accordo internazionale bilaterale con gli Stati Uniti per autorizzare le compagnie aeree a fornire i dati PNR alle agenzie statunitensi[198].

Con questo parere il Gruppo di lavoro ribadì innanzitutto il principio di finalità, quindi PNR possono essere usati solo per contrastare il terrorismo e non possono essere usati anche per altri sistemi quali ad esempio il CAPPS II. Un secondo punto era il principio di proporzionalità, proibendo la raccolta di informazioni eccessive e non pertinenti. Poi veniva ancora una volta sottolineata l'importanza che la conservazione fosse concessa per un periodo limitato di tempo. Un ulteriore punto esponeva il divieto di trattare dati sensibili. Infine vi doveva essere un esercizio del diritto degli interessati: è necessario che i passeggeri ricevano informazioni chiare in merito a chi userà i dati raccolti e per quali scopi

5.3 Il conflitto tra Commissione e Parlamento europei

Con la decisione 2004/535/EC del 14 maggio 2004[199] la Commissione accordava al programma PNR un livello di protezione conforme con gli standard richiesti dalla direttiva 95/45/CE.

Subito dopo, il 17 maggio 2004 il Consiglio delle Comunità europee con

[197] Dichiarazione d'intenti dell'Ufficio doganale e di protezione dei confini (Cbp) del Dipartimento per la sicurezza interna" del 12 gennaio 2004
[198] nota 191
[199] Decisione della Commissione del 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection, Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32004D0535&from=EN

la decisione 2004/496/CE[200] approva un accordo tra l'Unione Europea e gli Stati Uniti sul trattamento e trasferimento dei PNR[201].

Il Parlamento europeo si era espresso negativamente tuttavia nella decisione del Consiglio fu dichiarato che in base all'articolo 300, paragrafo 3 del trattato che istituisce la Comunità europea(TCE) il Parlamento non aveva espresso entro i termini fissati il suo parere, un parere comunque non vincolante.

Il Parlamento europeo aveva inoltre inviato alla Corte di giustizia delle Comunità europee una richiesta di parere al riguardo, registrata dalla cancelleria della Corte in data 21 aprile 2014. Il Consiglio però, temendo un parere negativo, si affrettò a concludere l'accordo e a quel punto il Parlamento dovette ritirare la propria domanda di parere in quanto la conclusione dell'accordo rendeva privo di oggetto tale richiesta[202].

Qualche mese più tardi il Parlamento europeo convinto dell'incompatibilità dell'accordo con la legislazione europea presentò in data 27 luglio 2004 due ulteriori ricorsi alla Corte di giustizia.

Nella causa C-318/04 Parlamento europeo contro Commissione delle Comunità europee, la Corte avrebbe dovuto valutare la decisione 2004/535/EC sull'adeguato livello di protezione nei dati trasferiti alle autorità

---

[200] Decisione del Consiglio del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti, Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:32004D0496&from=EN

[201] Accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (passenger name record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti

[202] Federico Casolari, 2008, *L'incorporazione del diritto internazionale nell'ordinamento dell'Unione europea,* Giuffré editore

di frontiera statunitensi[203].

Nella causa C-317/04 Parlamento europeo contro Consiglio dell'Unione europea, era obbiettivo del Parlamento ottenere l'annullamento della decisione 2004/496/CE e del conseguente accorto al trasferimento dei PNR con gli Stati Uniti[204].

Le sentenze della Corte di giustizia in merito ai ricorsi presentatati dal Parlamento europeo arrivarono nel maggio 2006.

Per quanto riguarda la prima causa, C-318/04 contro la decisione di adeguatezza della Commissione, i quattro motivi sollevati dal Parlamento sono (1) un eccesso di potere, (2) una violazione dei principi della direttiva 95/46/CE, (3) una violazione dei diritti fondamentali ed (4) una violazione del principio di proporzionalità[205].

Innanzitutto nel suo giudizio la Corte evidenziava che in base al secondo paragrafo dell'articolo 3 della direttiva 95/46/CE sono esclusi dalle sue sfere di applicazioni i casi di trasferimento di dati personali che effettuati per attività che non rientrano nell'ambito del diritto comunitario, ed in particolar modo quelli riguardanti la sicurezza pubblica, la sicurezza dello Stato, la difesa e altre attività dello Stato in materia di diritto penale[206].

La Corte nei sui 'considerando' aveva rilevato che la decisione di adeguatezza riguardava il solo trasferimento dei dati PNR alle autorità di frontiera americane, la Customs and Border Protection(CBP) e che tale trasferimento aveva luogo ai sensi di una legge americana. Tale legislazione era volta a migliorare la sicurezza del paese e regolare gli ingressi e le uscite

[203] Cause riunite C-317/04 e C-318/04 Parlamento europeo contro Consiglio dell'Unione europea e Commissione delle Comunità europee Consultabile su:
http://curia.europa.eu/juris/liste.jsf?language=it&num=C-317/04
[204] idem
[205] Conclusioni dell'avvocato generale Philippe Léger sulle cause riunite C-317/04 e C-318/04 presentate il 22 novembre 2005 Consultabile su
http://curia.europa.eu/juris/liste.jsf?language=it&num=C-317/04
[206] Sentenza del 30 maggio 2006, nota 203, punto 54

dagli Stati Uniti[207].

Sulla base di quanto enunciato finora la Corte nel suo giudizio aveva dichiarato che il trasferimento dei dati PNR, non avviene per motivi commerciale, come quelli per cui vengono inizialmente raccolti dalle compagnie aeree, bensì sono volti alla salvaguardia della pubblica sicurezza e per fini repressivi[208].

Vennero a quel punto riprese le motivazioni di una precedente sentenza, la sentenza "Lindqvist", nella quale la Corte aveva già preso in esame la portata dell'articolo 3 paragrafo 2 della direttiva 95/46/CE.
In quella sentenza il regime di trasferimento dei dati personali verso dei paesi terzi veniva definito come "*un regime speciale, implicante norme specifiche, che mira a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso i paesi terzi*" istituendo così "*un regime complementare al regime generale attuato dal capo II della suddetta direttiva, riguardante la liceità di trattamenti dei dati personali*"[209].

Trattandosi dunque di attività proprie di autorità statali, e non legate alle attività dei singoli, il trattamento di tali dati doveva essere escluso dalla sfera di applicazione della direttiva 95/46/CE[210].

Sulla base di ciò la Corte concludeva dando ragione al Parlamento europeo che sosteneva che la decisione della Commissione fosse stata adottata *ultra vires*, in violazione dell'articolo 3 paragrafo 2 della direttiva 95/46/CE, senza la necessità ulteriore di valutare gli altri motivi indicati dal Parlamento.
Viene dunque annullata la decisione di adeguatezza della Commissione in quanto esulava dalle competenze della direttiva[211].

---

[207] Sentenza del 30 maggio 2006, nota 203, punto 55
[208] Sentenza del 30 maggio 2006, nota 203, punto 57
[209] Sentenza "Lindqvist" del 6 novembre 2003, causa C–101/01, punto 63
[210] Lindqvist, nota 209, punto 43
[211] Sentenza del 30 maggio 2006, nota 203, punto 70

Per quanto riguarda la seconda causa, C-317/04 sono sei i motivi addotti dal Parlamento europeo contro la decisione del Consiglio. Queste sono: (1) una scelta errata dell'art. 95 CE come fondamento giuridico, (2) la violazione dell'articolo 300, paragrafo 3, secondo comma, CE, per via di una modifica della direttiva 95/46/CE, (3) una violazione del diritto alla tutela dei dati personali, (4) una violazione del principio di proporzionalità, (5) una motivazione insufficiente della controversa decisione, e (6) una violazione del principio di leale cooperazione stabilito all'articolo 10 CE[212].

Nelle sue argomentazioni il Parlamento esponeva il fatto che l'art. 95 CE non poteva costituire un fondamento giuridico per la decisione presa dal Consiglio in quanto quella non aveva ad oggetto e contenuto il funzionamento del mercato interno o la contribuzione all'eliminazione di ostacoli per la libera prestazione dei servizi. Le finalità della decisione erano invece di legittimare un trattamento dei dati personali imposto dalla legislazione americana. A ciò si aggiunge anche l'aggravante che il trattamento di dati ad oggetto dell'accordo con gli Stati Uniti sarebbe escluso dall'ambito di applicazione della direttiva[213].

Per il Consiglio l'accordo sul trasferimento dei PNR con gli Stati Uniti era volto al rispetto delle libertà e dei diritti fondamentali, ed in particolar modo la vita privata. In più avrebbe garantito la soppressione di eventuali distorsioni della concorrenza tra le compagnie aeree degli Stati membri, ed anche tra queste e altre compagnie di Stati terzi. Secondo il Consiglio le condizioni di concorrenza sarebbero infatti state falsate poiché solo alcune compagnie aeree avrebbero autorizzato le autorità statunitensi ad accede ai loro database[214].

La Commissione, a sostegno del Consiglio, riteneva necessario appianare le divergenze di diritto internazionale pubblico tra la normativa

[212] nota 205
[213] Sentenza del 30 maggio 2006, nota 203, punto 63
[214] Sentenza del 30 maggio 2006, nota 203, punto 64

dell'UE e le leggi statunitensi. Aggiungeva che l'art.95 CE fosse un fondamento normativo idoneo, in quanto l'accordo toccava la dimensione esterna della protezione dei dati personali all'atto del loro trasferimento interno alla Comunità. Una competenza esclusiva esterna a tal riguardo sarebbe stata fondata dagli artt. 25 e 26 della direttiva 95/46/CE. Infine, secondo la Commissione l'uso delle autorità statunitense dei dati non li sottraeva alla direttiva in quanto inizialmente la raccolta effettuata dalle compagnie aeree avveniva a fini commerciali[215].

La Corte con il suo giudizio si limitò a constatare che l'art.95 CE, letto assieme all'art.25 della direttiva 95/46/CE, non risultava idoneo a fornire le competenze necessarie a concludere l'accordo. Quest'ultimo infatti aveva ad oggetto lo stesso trasferimento di dati contenuto nella decisione di adeguatezza valutata in precedenza e quindi, come in quel caso, si tratta di un trasferimento di dati che va al di fuori dell'ambito di applicazione della direttiva.

Senza dunque la necessità di valutare anche gli altri motivi addotti dal Parlamento, la Corte concluse la sentenza con l'annullamento della decisione 2004/496 del Consiglio[216].

5.4 I successivi accordi sui PNR con gli Stati Uniti

Nel luglio 2007 venne raggiunto un accordo tra l'UE e gli Stati Uniti riguardo al trasferimento dei dati PNR[217], ma arrivò immediata una risoluzione

[215] Sentenza del 30 maggio 2006, nota 203, punto 65
[216] Sentenza del 30 maggio 2006, nota 203, punto 65
[217] Accordo sul trattamento e sul trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) da parte dei vettori aerei al Dipartimento per la sicurezza interna degli Stati Uniti (DHS) (Accordo PNR del 2007)

del Parlamento che ne criticava l'iter legislativo, nel quale non era stato richiesto il parere di quest'ultimo[218].

In seguito, dopo l'entrata in vigore del Trattato di Lisbona, il 1 dicembre 2009, cambiava un fattore molto importante: il consenso del Parlamento europeo diventava necessario all'approvazione dell'accordo, e questi domandava una maggiore attenzione alla protezione degli standard di protezione dei dati personali. Infatti in base all'articolo 218 TFUE l'approvazione del Parlamento europeo era una condizione necessaria per concludere accordi che riguardano settori in cui si applica la procedura ordinaria. Fa parte di essi, in seguito all'abolizione del sistema a tre pilastri prodotta dal Trattato di Lisbona, anche la cooperazione giudiziaria e di polizia.

Il 5 maggio 2010 il Parlamento adottava una risoluzione con la quale rinviava la sua votazione, necessaria all'approvazione dell'accordo del 2007, fino a quando le modalità d'uso dei dati PNR non fossero state conformi al diritto europeo e, in particolar modo, all'attenzione che quest'ultimo pone sulla salvaguardia del diritto alla protezione dei dati personali[219].
I requisiti richiesti dal Parlamento europeo riguardavano nello specifico, da una parte, una maggior osservanza della legislazione europea sulla protezione dei dati. Poi, la necessità di fornire una valutazione d'impatto sulla privacy prima di poter adottare qualsiasi misura al riguardo. Allo stesso tempo risultavano necessarie delle prove di proporzionalità volte a dimostrare l'insufficienza degli strumenti giuridici esistenti. Inoltre, come stabilito dalla decisione quadro del 13 giugno 2002 sulla lotta al terrorismo[220], vi doveva

[218] Di fatto l'accordo raggiunto nel 2007 restò in piedi in modo temporaneo fino al raggiungimento del successivo accordo nel 2012.
[219] Risoluzione del Parlamento europeo del 5 maggio 2010 sull'avvio dei negoziati per la conclusione di accordi sui dati del codice di prenotazione (PNR) con gli Stati Uniti, l'Australia e il Canada 2011/C 81 E/12 Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.CE.2011.081.01.0070.01.ITA&toc=OJ:C:2011:081E:TOC
[220] GU L 164 del 22.6.2002, pag. 3.

essere una limitazione rigorosa delle finalità e un uso dei dati PNR limitato a reati o minacce valutate caso per caso. Una limitazione era anche necessaria per quanto riguarda la quantità di dati raccolti. Nella sua risoluzione il Parlamento poneva anche un divieto allo studio di profili effettuato con l'estrazione di dati. Infine doveva essere assicurata una vigilanza giuridica e di controllo democratico[221].

Ripresi i negoziati la Commissione riproponeva nel novembre 2011 una nuova proposta di accordo al Parlamento[222].

Nell'aprile 2012 il Parlamento fu nuovamente chiamato a votare la nuova revisione dell'accordo antiterrorismo sul trasferimento di dati PNR e in quell'occasione la maggioranza parlamentare votò per l'approvazione dell'accordo, nonostante il parere negativo del Gruppo di lavoro articolo 29. Un peso rilevante in questa decisione, in controtendenza rispetto alle scelte precedentemente fatte dal Parlamento, è stato senz'altro quello delle pressioni politiche esercitate dagli Stati Uniti[223]. Il governo americano aveva infatti minacciato la sospensione dei viaggi senza visto negli Stati Uniti[224].

Il nuovo accordo è così entrato in vigore il 1 luglio 2012 e ha validità per sette anni.

L'accordo prevede che le autorità statunitensi conservino i dati PNR in un database per cinque anni. Trascorsi i primi sei mesi, le informazioni con cui è possibile l'identificazione diretta di un passeggero vengono mascherate e "de-personalizzate". Al termine dei cinque anni, i dati vengono spostati in una "banca dati inattiva" per ulteriori dieci anni, ma con requisiti di accesso più

---

[221] Risoluzione del Parlamento, nota 219

[222] Commissione europea, Proposta di decisione del Consiglio relativa alla conclusione dell'accordo tra gli Stati Uniti d'America e l'Unione europea sull'uso e sul trasferimento del codice di prenotazione (Passenger Name Record — PNR) al Dipartimento per la sicurezza interna degli Stati Uniti

[223] Resta, nota 95

[224] Ansa, 27 marzo 2012, *Terrorismo: Pe cede a Usa,ok a trasferimento dati passeggeri*, Consultabile su: http://www.ansa.it/europa/notizie/rubriche/altrenews/2012/03/27/visualizza_new.html_157702446.html

rigidi. Il fine dell'uso dei dati PNR deve essere quello di combattere il terrorismo e i reati transnazionali gravi.
I dati sensibili come credenze religiose ed origini etniche, che possono per esempio essere ricavati attraverso le scelte dei pasti per motivi religiosi, sono consentiti solo in casi eccezionali e vanno valutati caso per caso. Dovranno poi essere cancellati entro 30 giorni, a meno che non siano utilizzati per un'indagine in corso.
Infine i cittadini potranno accedere ad una modalità di ricorso secondo le leggi statunitensi[225].

Possiamo quindi rilevare che l'accordo del 2012 non soddisferebbe molte delle richieste che erano state poste dal Parlamento nella sua risoluzione del 2010. Più specificatamente, il periodo di conservazione dei dati non è stato ridotto ma resta invece molto lungo. I dati sono resi anonimi solo in parte. Nell'accordo il data mining e la "profilazione" della persone non vengono esplicitamente vietate.
Inoltre i diritti dei cittadini non sembrano essere salvaguardati in modo efficace: un individuo può richiedere i propri dati PNR dalle autorità americane ma nell'accordo non viene specificato gli obblighi di quest'ultime, che potrebbero declinare la richiesta.
Come più volte messo in evidenza dal Gruppo di lavoro artico 29, la Commissione non ha mai dato prova della necessità e proporzionalità delle misure adottate nell'accordo ai fini di combattere il terrorismo.
Infine l'accordo non sembra dare sufficienti garanzie al riguardo di trasferimenti verso paesi terzi[226].

L'accordo sembrerebbe dunque una vittoria di interessi politici a scapito

[225] Comunicati stampa del Parlamento europeo, 19 aprile 2012, "*Il Parlamento dà il via libera all'accordo con gli USA sui dati dei passeggeri aerei*, Consultabile su: http://www.europarl.europa.eu/news/it/news-room/20120419IPR43404/il-pe-d%C3%A0-il-via-libera-all'accordo-con-gli-usa-sui-dati-dei-passeggeri-aerei
[226] European digital rights, *Is the new EU-US PNR Agreement acceptable?* , Consultabile su: https://edri.org/files/2012EDRi_US_PNRcomments.pdf

del diritto alla protezione dei dati personali dei cittadini europei.

5.5 L'opposizione ad una direttiva europea sui PNR

Nel febbraio 2011 la Commissione presentava una proposta di direttiva sull'uso dei PNR per la lotta al terrorismo al riguardo di voli tra un paese terzo e uno Stato membro[227].

Il 5 aprile 2011 il Gruppo di lavoro ex art.29 ha prodotto un parere negativo al riguardo. Il Gruppo di lavoro valutava con criticità gli aspetti di necessità e proporzionalità che non arrivano a giustificare la limitazione dei diritti e delle libertà fondamentali.

Secondo il Gruppo di lavoro non vi sono prove che il trattamento dei dati PNR in tutti gli Stati membri eviterebbe falle nella sicurezza dovute all'abolizione delle frontiere interne.

Viene fatto notare che il trattamento dei dati PNR come strumenti di intelligence comporta anche un aumento dei livelli dei requisiti di garanzia richiesti nel campo della protezione dei dati. Andrebbe invece valutato se gli strumenti di cooperazione giudiziari non siano strumenti più adeguati per il medesimo fine.

Inoltre, raccogliere tutti i dati di tutte le persone sui voli è una misura sproporzionata che contrasta con l'articolo 8 della Carta dei diritti fondamentali[228].

---

[227] Proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi

[228] Gruppo di lavoro articolo 29 per la protezione dei dati, Parere 10/2011 sulla proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi adottato il 5 aprile 2011 Consultabile su: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp181_en.pdf

Nel giugno 2011 anche il Garante europeo della protezione dei dati (in seguito GEPD) diede il suo parere riguardo la proposta di direttiva della Commissione.

Il GEPD notava i progressi nel tentativo di limitare la sfera di applicazione della proposta e le condizioni di trattamento dei dati PNR. Tuttavia, il suo parere restava contrario in quanto i requisiti essenziali di necessità e proporzionalità non venivano soddisfatti. Riteneva nel suo parere che la rilevazione di dati PNR dovrebbe avvenire solo per casi specifici.

Altre carenze individuate dal GEPD sono il campo di applicazione eccessivamente vasto. La natura delle minacce che consentono lo scambio di dati dovrebbe essere definito in modo più chiaro. I dati andrebbero conservati in forma identificabile per un periodo non superiore a 30 giorni e poi mascherati. Ed infine all'interno dei dati PNR gli elementi trattati andrebbero ridotti[229].

Nell'aprile 2013 la commissione per le libertà civili, la giustizia e gli affari interni (LIBE) del Parlamento europeo rifiutò la proposta che era stata presentata nel 2011 dalla Commissione. La votazione vide 30 voti contro la proposta e 25 a favore.

La maggior parte dei membri del LIBE nella loro opposizione alla proposta riprendevano le motivazioni già espresse dal Gruppo di lavoro e dal Garante europeo della protezioni dei dati.

Nello specifico ponevano dei dubbi sulla proporzionalità della raccolta, uso e conservazione dei dati dei passeggeri di compagnie aeree previsti dalla direttiva proposta. A maggior ragione per il fatto che ciò avviene indifferentemente che un individuo sia o meno un sospetto. Viene sottolineato poi il fatto che non si accordi ai diritti fondamentali, in particolar modo quello

[229] Parere del Garante europeo della protezione dei dati sulla proposta di una direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi *(*Pubblicato sulla GUUE n. C 181 del 22.6.2011*)*

sulla protezione dei dati.
Dall'altra parte, le ragione di coloro del fronte minoritario che aveva votato in modo favorevole la proposta di legge davano risalto al potenziale valore aggiunto che tale direttiva avrebbe potuto portare ai fini del controterrorismo europeo. Aggiungendo inoltre che raggiungere un modello unico europeo sarebbe stata un'opzione migliore di quella in atto in quel momento, di singole diverse decisioni per ciascuno Stato membro[230].

5.6 La nuova direttiva europea sui PNR

Il dibattito al riguardo dei PNR si riaccese qualche tempo dopo, in particolare in riferimento alla possibile minaccia posta da europei che avrebbero potuto far ritorno a casa dopo aver combattuto all'estero per gruppi terroristici.
In questo contesto il Consiglio europeo sollecitò il Parlamento europeo a lavorare con celerità per raggiungere un accordo su una direttiva al riguardo dei PNR. Inoltre sottolineava l'importanza di lavorare un approccio che sia coerente con quelli adottati dai paesi terzi, e raccomandava dunque una stretta cooperazione[231].

Nel momento in cui la minaccia del terrorismo si materializzò effettivamente, con la sparatoria alla sede di Charlie Hebdo del 7 gennaio 2015[232], si fecero pesanti le pressione sui parlamentari europei affinché

[230] Conferenza stampa del Parlamento europeo, 24 aprile 2013 "Civil Liberties Committee rejects EU Passenger Name Record proposal" Consultabile su: http://www.europarl.europa.eu/news/en/news-room/20130422IPR07523/civil-liberties-committee-rejects-eu-passenger-name-record-proposal
[231] Riunione straordinaria del Consiglio d'Europa del 30 agosto 2014 Consultabile su: http://www.consilium.europa.eu/en/meetings/european-council/2014/08/30/
[232] vedi Attentato alla sede di Charlie Hebdo Connsultabile su: https://it.wikipedia.org/wiki/Attentato_alla_sede_di_Charlie_Hebdo

concludessero i lavori su una direttiva volta a regolare il trasferimento e il trattamento dei dati PNR. In modo particolare, i capi di Stato riuniti a Brussels il seguente 12 febbraio posero la direttiva sui PNR al primo posto delle necessità più immediate ed urgenti al fine di garantire la sicurezza dei cittadini[233].

Il 14 aprile 2016 il Parlamento europeo ha approvato la direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi.
A conclusione dell'iter, il testo è stato approvato dal Consiglio d'Europa il 21 aprile[234].

Per la salvaguardia del diritto fondamentale alla protezione dei dati personali sono poste alcune limitazioni al trasferimento, uso e conservazione dei dati personali. In primis, i dati PNR possono essere trattati solamente per indagini nella lotta al terrorismo o nei confronti di reati gravi. In secondo luogo, vengono vietati la raccolta ed il trattamento dei dati sensibili. Poi, è consentita la conservazione dei dati PNR fino ad un massimo di 5 anni, e dopo un periodo iniziale di 6 mesi devono essere mascherati e resi anonimi, in modo che l'individuo non possa essere identificato in modo diretto. Ciascuno Stato membro deve creare un'unità d'informazione dei passeggeri e dovranno inoltre essere trasparenti e dunque informare chiaramente i passeggeri della raccolta dei dati PNR. Infine un trasferimento dei dati PNR a dei paesi terzi va valutato caso per caso[235].

Sembra dunque che si sia ripetuto il caso eclatante del 2012 dove il Parlamento ha votato per ragioni politiche a favore di un accordo che non

[233] Riunione informale dei capi di Stato a Brussels il 12 febbraio 2015 Consultabile su: http://www.consilium.europa.eu/en/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/
[234] gli stati hanno ora due anni per conformarsi alla direttiva
[235] Consiglio europeo, Disciplina dell'uso dei dati del codice di prenotazione (PNR) Consultabile su: http://www.consilium.europa.eu/it/policies/fight-against-terrorism/passenger-name-record/

raggiungeva i requisiti da lui stesso richiesti in precedenza. Se allora furono le minacce statunitensi a costringere molti Parlamentari a cambiare il loro voto, in quest'occasione sono state le pressioni politiche provocate dalle paure che hanno attanagliato il vecchio continente di fronte alla scia di sangue iniziata dall'attentato alla sede di Charlie e che nei mesi seguenti ha macchiato di rosso altre strade della Francia e del Belgio.

Per alcuni, come il Garante europeo della protezione dei dati, si tratta di una misura invasiva e inefficace. Infatti secondo il garante della privacy Buttarelli negli attentati verificatisi negli ultimi due anni le informazioni erano già a disposizione delle autorità e il PNR non avrebbe potuto aggiungervi nulla. Oltre a sottolineare i costi elevati dell'operazione e i tempi molto lunghi che richiederà la sua messa in atto, critica il fatto che "troppe informazioni equivalgono a nessuna informazione"[236].

5.7 Alcuni cenni sull'annullamento della direttiva sulla conservazione dei dati e sulle conseguenze per gli accordi PNR

Infine può essere interessante e rilevante analizzare la vicenda dell'annullamento della direttiva sulla conservazione dei dati[237] da parte della Corte di giustizia e le sue conseguenze sull'accordo PNR con il Canada.

[236] Intervista dell'ANSA al Garante europeo della protezione dei dati Giovanni Buttarelli del 14 aprile 2016, Consultabile su:
http://www.ansa.it/europa/notizie/rubriche/altrenews/2016/04/14/garante-privacy-ue-pnr-e-infortunio-normativo_d9014be4-028e-477a-9479-18cc06f72d51.html

[237] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE. Dichiarata invalida l'8 aprile 2014 dalla sentenza dalla Corte di Giustizia UE

L'8 aprile 2014 la Corte di Giustizia ha dichiarato illegittima la direttiva 2006/24/CE in quanto violava il principio di proporzionalità nel rapporto tra il diritto alla protezione dei dati e le necessità di pubblica sicurezza[238].

La Corte aveva ricevuto delle domande pregiudiziali da parte della High Court irlandese e dal Verfassungsgerichtshof, la Corte costituzionale austriaca. La High Court era chiamata a valutare su una controversia aperta dalla società Digital Rights Ireland, contro le autorità irlandesi. Alla base della questione vi erano alcuni provvedimenti nazionali che recepivano la direttiva in materia di conservazione dei dati, ritenuti illegittimi dalla società irlandese. Nel caso austriaco, similmente, il governo del Land della Carinzia, assieme al signor Seitlinger e numerosi altri ricorrenti chiedevano alla Corte costituzionale l'annullamento di diverse disposizione interne che trasponevano la direttiva 2006/24/CE.

La Corte nella sua sentenza rilevava innanzitutto che la direttiva causava una vasta ingerenza nei diritti fondamentali al rispetto della vita privata e alla protezione dei dati personali della quasi totalità della popolazione europea[239]. Ciò contrasta con i rispettivi articoli 7 e 8 della CEDU, volti a tutelare tali diritti.

Poi la Corte ha ritenuto che se da una parte l'utilizzo di tali dati potesse essere giustificato dall'obiettivo che perseguiva di lotta alla criminalità grave e per ragioni di pubblica sicurezza, dall'altra parte ha ritenuto tuttavia che il legislatore nell'adottare la direttiva abbia ecceduto i limiti convenuti dal principio di proporzionalità[240].

In primo luogo, tale violazione al diritto di proporzionalità è motivato dalla Corte dal fatto che le misure di conservazione dei dati siano generalizzate e indifferenziate agli individui nel loro insieme e non sia invece stata attuata una più stretta limitazione che puntasse in modo preciso a perseguire la lotta

[238] Sentenza nella cause riunite C-293/12 e C-594/12 Digital Rights Ireland e Seitlinger e a. Consultabile su: http://curia.europa.eu/juris/liste.jsf?num=C-293/12&language=IT
[239] Sentenza cause riunite C-293/12 e C-594/12, nota 238, punto 56
[240] Sentenza cause riunite C-293/12 e C-594/12, nota 238, punto 69

contro i reati gravi[241].

In secondo luogo, il generico rinvio a “reati gravi” contenuto nella direttiva non specifica chiaramente i casi in cui le autorità possono accedere i dati e lascia spazio ad una libera interpretazione a ciascuno Stato membro sulla base del suo diritto interno[242].

In terzo luogo, riguardo alla durata della conservazione dei dati personali, la direttiva non prevede dei criteri che differenzino la durata della conservazione dei dati a seconda delle categorie di questi, ma si limita a stabilirne una durata minima di 6 mesi e massima di 24 mesi. Inoltre la direttiva omette di imporre che i dati così raccolti siano conservati solo nel territorio UE[243].

La sentenza dichiarando invalida la direttiva 2006/24/CE sceglie di valorizzare il diritto alla protezione dei dati personali anche in un ambito, quello della lotta alla criminalità grave, che consentirebbe una maggior limitazione delle libertà fondamentali in virtù delle esigenze a carattere generale. Una sentenza che si schiera contro la sorveglianza digitale di massa, in quanto la direttiva non era “mirata” e inoltre forniva alle autorità una possibilità di accesso indiscriminato.

Le conseguenze della sentenza citata pocanzi si sono estese anche all’accordo PNR che l’UE aveva stretto con il Canada.

Unione europea e Canada avevano iniziato a negoziare un accordo sul trasferimento dei dati PNR alle autorità canadesi al fine di combattere il terrorismo e i gravi crimini transnazionali. Questo accordo è stato infine firmato nel 2014, ma il Parlamento europeo prima di votare e approvare l’accordo ha deciso di adire la Corte di giustizia per sapere se nell’accordo vi era conformità con il diritto dell’UE. Più nello specifico il Parlamento richiede alla Corte come prima questione di valutare se l’ingerenza nel diritto alla

[241] Sentenza cause riunite C-293/12 e C-594/12, nota 238, punto 59
[242] Sentenza cause riunite C-293/12 e C-594/12, nota 238, punto 60
[243] Sentenza cause riunite C-293/12 e C-594/12, nota 238, punti 63, 63

protezione dei dati sia giustificabile e come seconda questione di valutare se l'accordo si fondi giuridicamente sugli articoli 82 e 87 TFUE(di cooperazione giudiziaria in materia penale e cooperazione di polizia) o invece sull'articolo 16 TFUE(sulla protezione dei dati personali)[244].

La Corte deve ancora esprimersi in merito ma l'8 settembre 2016 l'avvocato generale Mengozzi ha presentato le sue conclusioni, che pur non essendo vincolanti, propongono alla Corte una soluzione giuridica che molto spesso viene poi ripresa nella sentenza.

L'avvocato generale, seguendo usando in molti casi come metro di paragone la sentenza dell'8 aprile 2014, Digital Rights Ireland, giunge alla conclusione che l'accordo sul trasferimento di dati PNR tra UE e Canada non può essere raggiunto nella forma attuale[245].

L'avvocato generale ha infatti ritenuto che alcune disposizioni previste dall'accordo siano in contrasto con la carta dei diritti fondamentali dell'UE.

In primo luogo le autorità canadesi vengono autorizzate a conservare i dati PNR per un periodo massimo di cinque anni, per qualsiasi azione senza che vi sia richiesto un collegamento con le finalità perseguite. In questo caso, similmente alla causa Digital Rights Ireland, la necessità di conservare i dati per un periodo così lungo non è giustificato dalle due parti[246].

In secondo luogo, come nella causa Digital Rights Ireland, l'accordo "non specifica i criteri obiettivi in base ai quali sono individuati i funzionari che hanno accesso ai dati PNR". Ed inoltre l'accesso ai dati non è subordinato da un preventivo controllo di un'autorità indipendente[247].

---

[244] Riguardo alla seconda questione, nella quale non entrerò in merito in questa discussione, l'avvocato generale nelle sue conclusioni ha valutato che si fondi al tempo stesso sull'articolo 16 e 87 TFUE in quanto i due risultano in questo caso inscindibili e di pari importanza.

[245] Conclusioni dell'avvocato generale Paolo Mengozzi sulla domanda di parere 1/15 Consultabile su:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1#Footref105

[246] Conclusioni avvocato generale v. nota 245 (punti 274-282)

[247] Conclusioni avvocato generale v. nota 245 (punti 262-268)

Inoltre l'avvocato generale denota il mancato rispetto del criterio di necessità, così come più volte indicato anche dal Gruppo di lavoro articolo 29 e dal Garante europeo della protezione dei dati nei loro pareri e opinioni contrari ad accordi e direttiva sui PNR. L'accordo eccede la necessità in quanto vengono trasferiti anche dati delicati[248]. In più viene concesso al Canada di comunicare qualsiasi informazione anche se non per fini diversi da quelli previsti dall'accordo[249].

Spetterà tra qualche mese alla Corte informare il Parlamento europeo della sua decisione. Se la Corte darà ascolto all'avvocato generale dichiarando che l'accordo sui PNR con il Canada non può essere raggiunto, l'eco della sentenza potrebbe avere una successiva risonanza anche per l'accordo attualmente in vigore con gli Stati Uniti e per la neo-nata direttiva sull'uso dei dati PNR[250].

[248] Conclusioni avvocato generale v. nota 245 (punti 221-222)
[249] Conclusioni avvocato generale v. nota 245 (punto 80)
[250] alcuni parlamentari europei come Eva Joly ritengono che se i giudici seguiranno il parere dell'avvocato generale, a quel punto anche la direttiva sul PNR europeo verrà invalidata. Consultabile su: http://www.eunews.it/2016/09/08/avvocato-generale-corte-ue-boccia-pnr-tra-ue-e-canada-viola-diritti-fondamentali-ue/66561

Capitolo 6
SWIFT e le controversie del programma TFTP

6.1 Le origini della vicenda SWIFT

In seguito agli attentati terroristici dell'11 settembre 2001, l'amministrazione Bush si è mossa nella direzione di una maggiore sicurezza, da ottenere a tutti i costi.

Prima degli attacchi dell'11 settembre le autorità americane non avevano posto una profonda attenzione all'aspetto finanziario del terrorismo, in quanto i costi legati ad un attentato erano nella maggior parte dei casi molto bassi. Ciò cambierà dopo gli attentati. In seguito ad investigazioni gli inquirenti stimeranno il costo degli attentati alle Torri gemelle tra i 400.000 e 500.000 dollari. Di quella cifra, 300.000 dollari furono depositati nei conti correnti dei 19 dirottatori. Si tratta di movimenti di denaro ingenti che partivano dalla Germania, dagli Emirati Arabi Uniti, ma all'epoca i controlli erano focalizzati sul traffico di droga e i casi di frode finanziaria e le transazioni ai dirottatori passarono dunque inosservate nell'anonimità garantita dal sistema finanziario[251].

A quel punto il Governo statunitense cominciò a porre una maggior attenzione all'aspetto finanziario del terrorismo e il Dipartimento del Tesoro, con l'appoggio della CIA, dava inizio segretamente a un programma chiamato "Terrorist Finance Tracking Program" (in seguito TFTP). Grazie ad esso il

[251] J.Roth, D.Greenburg, S. Wille, Commissione 11 settembre, 2004, *Monograph on Terrorist Financing*

Dipartimento del Tesoro poteva raccogliere informazioni relative alla messaggistica finanziaria, in particolare l'identità di un ordinante e di un beneficiario di una transazione, ovvero il numero di conto, il nome, un indirizzo[252].

In particolare questi dati veniva presi da un database internazionale di transizioni finanziarie della Society for Worldwide Interbank Financial Telecommunications (SWIFT). La SWIFT è un consorzio europeo di istituzioni finanziarie creato nel 1973, con sede in Belgio. Non gestisce direttamente né denaro, né scambi monetari ma fornisce istruzioni criptate di trasferimento, servizi finanziari standardizzati e interfacce software per più di 8000 istituti finanziari in 206 differenti paesi. Viene inoltre supervisionato dalla Federal Reserve, dalla Banca centrale europea, dalla Bank of England, e dalla Bank of Japan[253]. SWIFT giornalmente indirizza in media 15 milioni transizioni tra banche, broker e istituti finanziari per una somma complessiva di all'incirca sei trilioni di dollari. Due terzi di questi sono originati in Europa[254].

Nel 2001 SWIFT conservava tutte le informazioni delle transizioni per un periodo di 124 giorni in due sedi, una nell'UE e una situata in Virginia, negli Stati Uniti, dove era presente una copia di tutti i dati collegati alle transizioni. Grazie alla presenza dei server situati fisicamente nel suolo americano, il Dipartimento del Tesoro fece valere i suoi poteri per accedere alle informazioni contenute in quegli archivi digitali.

[252] David B. Bulloch, 2011, *Tracking terrorism finances: the 'swift' program and the american anti-terrorist finance regime*, Amsterdam Law Forum
[253] SWIFT, About Us https://www.swift.com/about-us
[254] Bulloch, nota 252

6.2 Riflettori accesi sul programma TFTP

Nel 2006 due giornalisti del New York Times furono i primi a pubblicare un articolo che rivelava il programma di contro-terrorismo e nel quale svelava il trasferimento di dati personali in corso dal centro operativo della SWIFT al Dipartimento del Tesoro americano [255]. Il TFTP non si limitava ad un controllo dei flussi internazionali, ma qualsiasi operazione, a partire da un semplice prelievo ATM, veniva posta sotto la lente da parte dei servizi di intelligence americana.

Alcuni membri dell'amministrazione Bush difesero subito a spada tratta il programma, definendolo un tassello essenziale della lotta al terrorismo. Inoltre enunciavano alcuni successi nella lotta al terrorismo ottenuti grazie ai dati ottenuti nei SWIFT: la cattura di Hambali, artefice dell'attentato ad un resort di Bali nel 2002 e l'arresto di un residente di Brooklyn, Uzair Parchara, accusato di aver finanziato dei membri di Al Qaeda in Pakistan attraverso riciclaggio di denaro in una banca di Karachi[256].

Se negli Stati Uniti l'opinione pubblica era ormai stata abituata a misure drastiche di riduzione della privacy per favorire un aumento dei controlli anti terrorismo, pesante fu la ricezione di queste notizie in Europa.

Dal canto suo il CEO di SWIFT si affrettò subito a rilasciare una dichiarazione nella quale diceva di aver rispettato la normativa sulla protezione dei dati[257].

Nel frattempo nel polverone finì la BCE, che avendo il ruolo di supervisore della SWIFT veniva accusata di essere al corrente dei fatti e di non aver fatto nulla per proteggere la privacy dei cittadini.

---

[255] Lichtblau & Risen, 23 giugno 2006 '*Bank Data is Sifted by US in Secret to Block Terror', New York Times*, Consultabile su: http://www.nytimes.com/2006/06/23/washington/23intel.html

[256] Patrick M. Connorton, 2007, *Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide*, 76 Fordham L. Rev. 283 Consultabile su: http://ir.lawnet.fordham.edu/flr/vol76/iss1/7

[257] SWIFT, 23 giugno 2006, SWIFT statement on compliance policy. Consultabile su: https://www.swift.com/insights/press-releases/swift-statement-on-compliance-policy

Jean-Claude Trichet fece allora una dichiarazione di fronte al Parlamento europeo nella quale da una parte portava in sua difesa gli accordi di confidenzialità che erano stati stretti con la SWIFT e dall'altra la mancanza di autorità e poteri per poter regolare la protezione dei dati personali[258].

La Commissione europea intanto aveva incaricato l'autorità di controllo della tutela dei dati personali belga di indagare sulla questione.

Il Garante belga innanzitutto categorizzò la SWIFT come un "titolare del trattamento di dati personali" e non come un "responsabile del trattamento" e ciò lo poneva sotto maggiori responsabilità per le violazioni della privacy sotto la legge belga. Come titolare del trattamento di dati personali aveva mancato di informare gli interessati che stava fornendo dati finanziari agli Stati Uniti, venendo meno ad un suo dovere legale. In più, la SWIFT aveva commesso una grave violazione in quanto al trasferimento di dati personali in un Paese terzo non provvisto di un'adeguata tutela dei dati personali[259].

Due mesi dopo il parere dell'Autorità belga anche il Gruppo di lavoro Articolo 29 emise il suo parere e similmente al primo parere dichiarava che la SWIFT era venuta meno al suo dovere di fornire informazioni, di notificare gli interessati del trattamento dei dati personali e di fornire un appropriato livello di protezione a quei dati. Concluse dichiarando che il trasferimento segreto, sistematico, massiccio e a lungo termine di dati personali dalla SWIFT al Dipartimento del Tesoro, che avveniva in modo confidenziale, senza trasparenza e senza il controllo indipendente di un'autorità che supervisioni la protezione dei dati personali, costituiva una violazione dei principi fondamentali dell'Unione europea in materia di protezione dei dati personali e

[258] Discorso di Jean-Claude Trichet, Presidente della BCE al Parlamento europeo del 4 ottobre 2006. Consultabile su: https://www.ecb.europa.eu/press/key/date/2006/html/sp061004.en.html
[259] Commission de protection de la vie privée, 26 settembre 2006, Opinion on the transfer of personal data by the CSLR SWIFT by virtue of UST (OFAC) subpoenas. Consultabile su: http://www.steptoe.com/assets/attachments/2644.pdf

non è in accordo con le leggi belga ed europee. Infine richiedeva alla SWIFT di interrompere il trasferimento fuorilegge di dati[260].

La SWIFT si trovò a quel punto in un fuoco incrociato, chiusa da una parte dalle pressioni americane che minacciavano pesanti sanzioni nel caso di mancata acquisizione delle informazioni e il diritto dell'Unione europea che vietava tale trasferimento.

Stati Uniti e Unione europea trovarono un accordo temporaneo nel giugno 2007 in base al quale le informazioni ottenute dalla SWIFT potevano essere usate solamente al fine di combattere il terrorismo e i suddetti dati potevano essere conservati per al più cinque anni. Veniva inoltre previsto che degli osservatori europei monitorassero il programma[261].

6.3 L'accordo temporaneo sui TFTP

L'accordo temporaneo aveva trovato una soluzione accettabile per le parti, ma la situazione cambiò alla fine del 2009. La SWIFT decise di spostare i suoi server dagli Stati Uniti alla Svizzera e dunque, a partire da quel momento, gli Stati Uniti non hanno più avuto accesso ai dati della società belga.

La Commissione europea e i rappresentanti degli Stati Uniti iniziarono allora a lavorare ad un accordo *ad interim* per fornire agli Stati Uniti l'accesso ai dati SWIFT.

[260] Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Consultabille su: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2006/wp128_en.pdf
[261] Connorton, nota 256

L'accordo prevedeva che gli Stati Uniti potessero ottenere dalla società belga informazioni relative al nome, al numero di conto, all'indirizzo e ad altri dati personali che sarebbero poi stati usati dalle autorità americane esclusivamente in investigazioni connesse alla lotta al terrorismo. Inoltre la richiesta statunitense di informazione doveva essere il più possibile precida in modo da trasferire solo i dati strettamente necessari. I dati sarebbero stati conservati per cinque anni e non potevano essere trasferiti a paesi terzi. Infine non potevano essere monitorate le transazioni interne a Stati membri dell'Unione europea.

L'accordo ad interim è stato firmato dal Consiglio accorciando il più possibile le tempistiche e facendo in modo che ciò avvenisse prima del 1 dicembre 2009, quando sarebbe entrato in vigore il Trattato di Lisbona, che avrebbe reso necessario per l'accordo anche l'ulteriore approvazione del Parlamento. Come una beffa per il Parlamento, recava la data del 30 novembre 2009 la decisione del Consiglio che autorizzava l'accordo provvisorio[262].

Con l'entrata in vigore del Trattato di Lisbona il Parlamento europeo guadagnava il diritto di approvare o rifiutare gli accordi internazionali. In virtù di ciò, l'11 febbraio, il Parlamento ha votato una risoluzione per respingere l'accordo provvisorio sul trasferimento dei dati bancari agli Stati Uniti con la rete SWIFT, che è stata approvata con 378 voti favorevoli, 196 contrari e 31 astensioni. Le ragioni del voto sono motivate principalmente da preoccupazioni legate alla privacy e ad una mancanza di proporzionalità e reciprocità dell'accordo[263].

---

[262] Decisione 2010/16/PESC/GAI del Consiglio del 30 novembre 2009 relativa alla firma, a nome dell'Unione europea, dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi. Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=uriserv:OJ.L_.2010.008.01.0009.01.ITA&toc=OJ:L:2010:008:FULL

[263] Comunicato stampa del Parlamento europeo, 10 febbraio 2016, SWIFT: il Parlamento europeo boccia l'accordo con gli USA. Consultabile su:

In particolare una grave carenza dell'accordo è dovuta ai poco chiari confini del termine 'terrorismo' nella legislazione statunitense e che comportava quindi comportava un trasferimento di dati molto superiore a quello che potrebbe essere ritenuto necessario secondo standard europei[264]. Va inoltre considerato che vi è una grande differenza rispetto all'accordo raggiunto sui PNR, ovvero che in questo caso non vi è un collegamento diretto tra gli Stati Uniti e i dati trattati.

6.4 L'accordo sui TFTP

In seguito al rifiuto del Parlamento europeo, Stati Uniti ed Unione europea dovettero tornare a rinegoziare un accordo.

Arrivava così il 15 giugno 2010 una proposta di accordo da parte della Commissione, rinominata "TFTP II".

In base alla proposta di accordo tra i miglioramenti previsti vi erano il fatto che i cittadini europei avrebbero avuto possibilità di effettuare ricorsi nei tribunali statunitensi competenti e le richieste di trasferimento dei dati avrebbero prima dovuto ottenere l'approvazione dell'Europol,

Il 22 giugno il Garante europeo della protezione sui dati forniva il suo parere sull'accordo e notava miglioramenti rispetto al precedente[265]. In particolare la definizione di terrorismo veniva limitata ed avvicinata a quella

---

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//IT

[264] Els De Busser, 2012, *The Adequacy of an EU-US Partnership* in Serge Gutwirth e altri, European Data Protection: In Good Health?

[265] Parere del Garante europeo della protezione dei dati 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'U nione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II)

europea contenuta all'articolo 1 della decisione quadro del Consiglio del 13 giugno 2002 sulla lotta contro il terrorismo.
Tra i punti critici dell'accordo vi sono il trasferimento di dati in massa, che rimane presente anche nella nuova proposta[266].
Sembra poi eccessiva la conservazione di "dati non estratti", definizione peraltro vaga e priva di spiegazione, per un periodo di 5 anni. Peraltro, in una sentenza del 2 marzo 2010 la Corte costituzionale federale tedesca aveva ritenuto eccessiva la conservazione di dati sulle telecomunicazioni per un periodo di 6 mesi[267].
Poi delle critiche segnano la supervisione affidata all'Europol, che in primis non è un' autorità giudiziaria e in secondo luogo potrebbe avere a sua volta interessi dallo scambio di dati[268]. Infine i diritti degli interessati dovrebbero essere stabili in modo più chiaro[269].

Nonostante tutto, l'8 luglio 2010 il Parlamento europeo ha infine approvato il nuovo accordo TFTP II e il 13 luglio il Consiglio ha dato la sua approvazione, portando all'entrata in vigore dell'accordo il 1 agosto 2010.
I principali punti dell'accordo sono i seguenti:
In base all'articolo 4 le richieste di dati a fini della lotta al terrorismo devono essere il più possibile specifiche e necessarie. Tali richieste saranno valutate dal Europol.
L'articolo 5 specifica che i dati, una volta ricevuti, non potranno essere inseriti in ulteriori database o sfruttati per altri fini quale ad esempio la profilazione.
L'articolo 6 stabilisce che dati non più necessari devono essere rimossi. I 'dati non estratti' possono essere conservati per non più di 5 anni.
L'articolo 7 limita invece le possibilità di trasferimento successivo.

[266] nota 265, punti 19-20
[267] nota 265, punti 21-22
[268] nota 265, punti 23:27
[269] nota 265, punto 44

Nel complesso l'accordo non ha tenuto particolarmente conto delle critiche del Parlamento rivolte al primo accordo TFTP, né a quelle poste dal GEDP nel suo parere. Soprattutto per quanto riguarda il trasferimento di massa, non vi è stato un significativo miglioramento che lo proibisca: moltissimi nomi vengono trasferiti su liste anti terrorismo senza prove specifiche. Inoltre il tempo di conservazione dei dati resta molto elevato[270].

Da più parti si sono levate critiche per il ruolo di controllo che non è stato assegnato ad un'autorità giudiziaria indipendente, bensì all'Europol, ovvero un organismo di polizia che non si fa problemi ad approvare le richieste orali statunitensi e che ha vantaggi esso stesso dai trasferimento. La Parlamentare Sarah Ludford ha definito la situazione come "mettere di guardia la volpe nel pollaio"[271]. Bisogna tuttavia notare che l'operato dell'Europol viene a sua volta supervisionato dall' 'Autorità di controllo comune dell'Europol' che è formata dai rappresentati di tutte le autorità nazionali di controllo sui dati personali.

La vicenda SWIFT e gli accordi per il programma TFTP rappresentano l'ennesima riprova della differenza di vedute tra le due sponde dell'Atlantico: quella americana disposta a tutto per ottenere quantità infinite di dati da analizzare e incrociare, poiché quella sembra essere l'unica soluzione possibile per la prevenzione del terrorismo, e dall'altra parte quella europea che tiene maggiormente al rispetto della privacy dei suoi cittadini e che ritiene vi siano soluzioni meno invasive per ottenere altrettanti risultati nella lotta al terrorismo.

---

[270] Sylvia Kierkegaard, 2011, *US War on terror EU swift (ly) signs blank cheque on EU data* , Elsevier Ltd

[271] Comunicati stampa del Parlamento europeo, 16 novembre 2011, SWIFT implementation report: MEPs raise serious data protection concerns, Consultabile su: http://www.europarl.europa.eu/news/en/news-room/20110314IPR15463/swift-implementation-report-meps-raise-serious-data-protection-concerns

Conclusioni

Questa tesi non fotografa e non può fotografare un punto di arrivo nella materia della protezione dei dati personali. Questo elaborato piuttosto può mostrare un processo in continua evoluzione, che è tutt'oggi in atto.

Negli ultimi decenni in Europa sono stati compiuti enormi progressi sul piano della tutela del diritto alla protezione dei dati personali. In particolare, il nuovo Regolamento che entrerà in vigore nel 2018 renderà senza alcun dubbio la legge sulla privacy europea la più avanzata del mondo[272]. In particolar modo, per quanto riguarda le nuove tecnologie digitali, viene scelto in termini assoluti un orientamento alla privacy, come ad esempio la "privacy by design", che prevede che fin dalla progettazione di nuovi software l'attenzione deve essere portata ad uno sviluppo che tuteli la privacy dell'individuo.

Tuttavia i risultati raggiunti in Europa sono unici nel mondo e in un mondo dove gli scambi di dati e informazioni è sempre più massiccio e veloce, occorre tutelare i dati dei cittadini europei anche una volta varcate le frontiere del Vecchio Continente. Molti autori infatti si sono espressi promuovendo l'importanza di adottare regole comuni a livello internazionale, in modo da poter proteggere efficaciemente la privacy e i dati personali in un mondo sempre più globalizzato. I progressi finora sono stati pochi: per esempio, si può registrare che nel 2001 è stata aperta alla firma la Convenzione sulla criminalità informatica, risultato dei lavori del Consiglio d'Europa e ad oggi sono parte al trattato 49 stati membri, tra i quali anche

[272] Intervista a Giovanni Buttarelli (GEPD) di Francesca De Benedetti per Repubblica. Consultabile su: http://www.repubblica.it/tecnologia/2016/04/14/news/privacy_buttarelli-137648874/

Stati Uniti, Canada e Giappone[273]. Ciò dimostra che anche in ambito informatico è possibile trovare soluzioni accettate da una varietà di parti.

Nel frattempo, finché la privacy non trova un'intesa a livello mondiale, l'Europa si è tutela con l'articolo 25 della Direttiva 95/46/CE, che sarà rimpiazzato dall'articolo 45 della RGPD, che riguarda la richiesta un livello "adeguato" di protezione dei dati personali nel caso di trasferimento ad uno stato terzo, per rendere possibile il flusso di dati nella sua direzione. Ma finora la Commissione ha riconosciuto solamente ad 11 nazioni un adeguato livello di protezione. Ciò influirebbe negativamente negli scambi commerciali mondiali, per cui vengono raggiunti accordi ad hoc per permettere comunque il trasferimento di dati anche in paesi terzi sprovvisti di un adeguato livello di tutela. Raggiungere un accordo che possa soddisfare adeguatamente entrambe le parti non è mai facile, come ha dimostrato la travagliata vicenda dell'accordo Safe Harbour, poi sostuito dal Privacy Shield. Questo è anche l'accordo usato dai giganti dell'informatica statunitensi per vendere commercialmente i dati di milioni di utenti e generare da questi profitti astronomici.

Il rapporto tra i colossi dell'informatica statunitensi, come Facebook e Google, non è mai stato dei migliori. Proprio in questi giorni il Garante della privacy italiano ha iniziato a investigare sul trasferimento di informazioni che sta avvenendo da Whatsapp a Facebook. Uno scambio "interno" che avviene in virtù dell'acquisizione avvenuta nel 2014, ma la cui informativa resta molto vaga e non fa neppure seguire una richiesta di consenso, allertando così i controlli del Garante.

Un altro aspetto poco gradito alle aziende del mondo digitale statutinitense è

[273] Convenzione sulla criminalità informatica. Apertura del trattato a Budapest il 23 novembre 2001, aperto alla firma degli Stati membri e degli Stati non membri i quali hanno partecipato alla sua elaborazione e all'adesione degli altri Stati non membri. Entrato in vigore 1 luglio 2004 con 5 Ratifiche inclusi almeno 3 Stati membri del Consiglio d'Europa. Per l'Italia è entrato in vigore l'1 ottobre 2008 in seguito alla ratifica del 5 giugno 2008.

il “diritto all’oblio”, che richiede loro ogni giorno una dose extra di lavoro per rispondere alle richieste europeee di de-indicizzazione. Proprio per questo dovrebbero modificare la loro struttura prevedendo una maggior tutela della privacy fin dall’inizio, ed è ciò che ha pensato il legislatore pensando alla “privacy by design”. Ma in America il rispetto della privacy non è sentito con forza come in Europa, dove invece la storia di regimi totalitari ha insegnato una lezione importante. Sulla partita del diritto all’oblio si attende ora la sentenza della Conseil d’État.

Infine è importante che la lotta al terrorismo non diventi una scusa per attuare indiscriminatamente politiche di sorveglianza di massa, come quelle adottate fino a pochi anni fa dall’NSA, che non solo spiavano i propri concittadini, ma, quel che è peggio, spiavano alcuni leader europei come Angela Merkel e sedi di organismi internazionali come l’ONU.
Privare un individuo di una propria sfera di riservatezza equivale ad applicare un condizionamento costante del suo comportamento e privarlo delle sue libertà fondamentali.

Il mondo non è fatto in bianco e nero ma ci sono tutta una serie di gradazioni: così anche tra privacy e misure di sicurezza va ricercato il giusto bilanciamento. Le misure che negli anni scorsi gli Stati Uniti hanno messo in atto sono inaccettabili per un Paese democratico. Una politica di sorveglianza di massa è uno strumento che ricorda molto di più i sistemi adottati dai regimi totalitari, nei quali era necessario avere un controllo assoluto sull’individuo.

Il fatto che certe tecnologie siano disponibili non vuol dire che uno Stato debba ritenere di doverle usare. Non può mai essere permessa un’ingerenza incontrollata nella vita privata delle persone.
È indubbia la necessità di sicurezza, tuttavia raccogliere enormi quantità di dati è una pratica per lo più inutile, costosa e che non garantisce neppure risultati di successo. Uguali risultati possono essere ottenuti attraverso misure più circoscritte, più economiche e che siano meno invasive della privacy.

Basti pensare che gli ultimi attentati sono stati compiuti da “domestic fighters”, già noti alla polizia e i cui spostamenti erano già stati seguiti.

Anche qui la questione è ancora molto aperta e la sentenza della CGUE sul caso dell’accordo con il Canada per il trasferimento dei dati contenuti nei PNR avrà molto peso nel bilanciamento tra privacy e sicurezza.

L’Unione europea sta vivendo in questi giorni forse il periodo più buio della sua storia, ma ciò che non deve assolutamente fare è rinnegare la sua storia e i valori che incarna. In questo momento il rischio di smarrire la strada è grande, ma dovrà essere fatto uno sforzo da parte di tutti perché l’UE possa restare fedele a sé stessa e ai valori di libertà che vengono ritenuti fondamentali.

Bibliografia

Testi:

Dizionario Devoto-Oli Digitale 2016

Jon D. Mikalson, 2009, *Ancient Greek Religion,* Wiley-Blackwell

Hannah Arendt, 1958, *Vita activa: la condizione umana*, Bompiani

Gloria González Fuster, 2014, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer

Dorothy J. Glancy, 1979, *The invention of the right to privacy*, Arizona Law Review

William Faulkner, 1955, *Privacy*, Piccola Biblioteca Adelphi

Neil M. Richards e Daniel J. Solove, 2010, *Prosser's Privacy Law: A Mixed Legacy*, 98 Cal. L. Rev. 1887

Hannah Arendt, 1948, *Le origini del totalitarismo*, Piccola biblioteca Einaudi

George Orwell, 1949, *1984*, Mondadori

Finn, Wright, and Friedewald, 2013, *Seven types of privacy* in S. Guthwirth e altri, European Data Protection: Coming of Age, Springer

Stefano Rodotà, 2009, *Data Protection as a Fundamental Right* in S. Guthwirth e altri, Reinventing Data Protection?, Springer

De Hert e Gutwirth, 2009, *Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation* in S. Guthwirth e altri, Action in Reinventing Data Protection?, Springer

Lee A. Bygrave and Dag Wiese Schartum, 2009, *Consent, Proportionality and Collective Power* in Reinventing Data Protection?, Springer

Jan Berkvens, 2009, *Role of Trade Associations: Data Protection as a Negotiable Issue* in S. Guthwirth, Reinventing Data Protection?, Springer

Serge Gutwirth, 23 marzo 2011, *Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment*, ("Trade-offs and balancing" pp. 26-43) progetto PRESCIENT
Diana Alonso Blas, 2009, *First Pillar and Third Pillar: Need for a Common Approach on Data Protection?* in S. Guthwirth e altri, Reinventing Data Protection?, Springer

Chandler Jennifer, 2009, *Privacy versus national security: Clarifying the Trade-off*, in Kerr, Lucock e Steeves , Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society, Oxford University Press

Aquilina, Kevin, 2 marzo 2010, *Public security versus privacy in technology law: A balancing act?*, Computer Law & Security Review, Vol. 26, No. 2

G. Valkenburg, 2014, *Privacy Versus Security: Problems and Possibilities for the Trade-Off Model* in S. Gutwirth e altri, Reforming European Data Protection Law, Law, Governance and Technology Series 20

Ivan Szekely, 2009, *Freedom of Information Versus Privacy: Friends or Foes?* in Reinventing Data Protection?, Springer

Mayer-Schönberger, 2009, *Delete: The virtue of forgetting in the digital age*, Princeton: Princeton University Pres

P. Gianniti, 2015, *La CEDU e il ruolo delle corti*, Zanichelli

Marsha Cope Huie, Stephen F. Laribee, Stephen D. Hogan, 2002, *The right to privacy in personal data: the EU prods the US and controversy continues*, Tulsa Journal of Comparative and International Law, Vol. 9 Issue 2

Francesce Bignami, 2007, *European versus american liberty: a comparative privacy analysis of antiterrorism data mining*, Boston College Law Review Vol. 48:609

Shaman, Jeffrey M., 2006, *The right of privacy in state constitutional law,* Rutgers Law Journal, Issue 4, Vol. 37, p. 971-1085

Coles T.R., 1991, *Does the privacy act of 1974 protect your right to privacy?*, The american university law review, Vol.40:957

R. LeRoy, F.B. Cross, 1996, *The legal environment today*, Miller Business Law

P. Swire, S. Bermann, 2007, *Information privacy*, IAPP Publication

M.P. Eisenhauer, 2008, *The IAPP Information Privacy Case Book*, IAPP Pubblication

Rosen, 2012, *The right to be forgotten*, Stanford law review online

Zittrain, 2008, *The Future of the Internet and How to Stop It*, Yale University Press & Penguin UK 2008

G. Resta, V. Zeno-Zencovich, 2015, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma TrE-Press

Olga Mironenko, 2010, *Air Passenger Lists in Civil Aviation*, Kapittel 11

David H. Holtzman, 2006, *Privacy Lost: How Technology Is Endangering Your Privacy*, Jossey-Bass

Timothy M. Ravich, 2007, *Is Airline Passenger Profiling Necessary?,* 62 U. Miami L. Rev. 1

Bart Van Vooren, Ramses A. Wessel, 2014, *EU External Relations Law: Text, Cases and Materials,* Cambridge University Law

Federico Casolari, 2008, *L'incorporazione del diritto internazionale nell'ordinamento dell'Unione europea,* Giuffré editore

J.Roth, D.Greenburg, S. Wille, Commissione 11 settembre, 2004, *Monograph on Terrorist Financing*

David B. Bulloch, 2011, *Tracking terrorism finances: the 'swift' program and the american anti-terrorist finance regime*, Amsterdam Law Forum

Patrick M. Connorton, 2007, *Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide*, 76 Fordham L. Rev. 283

Els De Busser, 2012, *The Adequacy of an EU-US Partnership* in Serge Gutwirth e altri, European Data Protection: In Good Health?

Sylvia Kierkegaard, 2011, *US War on terror EU swift (ly) signs blank cheque on EU data* , Elsevier Ltd

Articoli online:

Keith Stuart and Charles Arthur, 27 aprile 2011, *PlayStation Network hack: why it took Sony seven days to tell the world*, The Guardian, Consultabile su: https://www.theguardian.com/technology/gamesblog/2011/apr/27/playstation-network-hack-sony

Stefano Rodotà, 23 ottobre 2011, *L'ansia di sicurezza che cancella i diritti*, articolo su La Repubblica, Consultabile su: http://www.repubblica.it/online/speciale/ventitreottobredue/ventitreottobredue/ventitreottobredue.html

Roger Clarke, 1997, *Introduction to Dataveillance and Information Privacy, and Definitions of Terms*, Xamax Consultancy, Consultabile su: http://www.rogerclarke.com/DV/Intro.html

Stefano Rodotà, 16 settembre 2004, Discorso conclusivo della Conferenza internazionale sulla protezione dei dati: *Privacy, libertà e dignità*

Intervista a Stefano Rodotà del 12 marzo 2016 a Linkiesta, Consultabile su: http://www.linkiesta.it/it/article/2016/03/12/stefano-rodota-la-trasparenza-totale-e-unidea-da-dittatori/29592/

Polly Sprenger, 26 gennaio 1999, *Sun on Privacy: 'Get Over It'*, Wired, Consultabile su: http://archive.wired.com/politics/law/news/1999/01/17538

Bobbie Johnson, 11 gennaio 2010, *Privacy no longer a social norm, says Facebook founder*, Consultabile su: https://www.theguardian.com/technology/2010/jan/11/facebook-privacy

Kuneva M., 2009, *European consumer commissioner, keynote speech, roundtable on online data collection, targeting and profiling* (Brussels). Consultabile su: http://europa.eu/rapid/press-release_ SPEECH-09-156_en.htm

Eric Schmitt e Thom Shanker, 26 luglio 2005, *U.S. Officials Retool Slogan for Terror War,* Consultabile su: http://www.nytimes.com/2005/07/26/politics/us-officials-retool-slogan-for-terror-war.html

Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark, 29 giugno 2013, *NSA Spied on European Union Offices*, Der Spiegel Consultabile su: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html

Pizzetti F.*, Il percorso del Consiglio d'Europa che porta al riconoscimento del diritto alla protezione dei dati personali*, LUISS, Consultabile su: http://docenti.luiss.it/privacy-pizzetti/tutela-e-protezione-dei-dati-personali-2/sintesi-lezione-6-ottobre-2010/

Dipartimento di Giustizia degli Stati Uniti, *What is FOIA?* , consultabile su: https://www.foia.gov/about.html

Rosen, J. ,21 luglio 2010, *The web means the end of forgetting*, The New York Times, Consultabile su: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all

Guido Scorza, 9 ottobre 2015, *Costeja Gonzalez: negato l'oblio all'uomo che lo ha regalato all'Europa*, Il fatto quotidiano, Consultabile su: http://www.ilfattoquotidiano.it/2015/10/09/costeja-gonzalez-negato-loblio-alluomo-che-lo-ha-regalato-alleuropa-2/2111057/

Commission nationale de l'informatique et des libertés, 12 giugno 2015, *CNIL orders Google to apply delisting on all domain names of the search engine*, Consultabile su: https://www.cnil.fr/fr/node/15790

Commission nationale de l'informatique et des libertés, 24 marzo 2016, *Right to be delisted: the CNIL Restricted Committee imposes a €100,000 fine on Google*, Consultabile su: https://www.cnil.fr/en/right-be-delisted-cnil-restricted-committee-imposes-eu100000-fine-google

Lucie Ronfaut, 19 maggio 2016, *Google affronte la Cnil devant le Conseil d'État sur le droit à l'oubli*, LeFigaro, Consultabile su http://www.lefigaro.fr/secteur/high-tech/2016/05/19/32001-20160519ARTFIG00142-google-affronte-la-cnil-devant-le-conseil-d-etat-sur-le-droit-a-l-oubli.php

Hugh Tomlinson, 18 luglio 2016, *Case Law, Belgium: Olivier G v Le Soir. "Right to be forgotten" requires anonymisation of online newspaper archive***,** Inform's blog, Consultabile su: https://inforrm.wordpress.com/2016/07/19/case-law-belgium-olivier-g-v-le-soir-right-to-be-forgotten-requires-anonymisation-of-online-newspaper-archive-hugh-tomlinson-qc/

Information Commissioner's Office, *Enforcement notice*, Consultabile su: https://ico.org.uk/media/action-weve-taken/enforcement-notices/1560072/google-inc-enforcement-notice-102015.pdf

Garante della privacy, Newsletter n. 397 del 22 dicembre 2014 Consultabile su: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3623678#1

Kathleen Miles, 24 novembre 2013, *Teens Get Online 'Eraser Button' With New California Law, Huffington Post*, Consultabile su: http://www.huffingtonpost.com/2013/09/24/teens-online-eraser-button-california_n_3976808.html

Gregory Ferenstein, 24 settembre 2013, *On California's bizzare Internet eraser law for teenagers*, Techcrunch, Consultabile su: https://techcrunch.com/2013/09/24/on-californias-bizarre-internet-eraser-law-for-teenagers/

Decisione della commissione sul livello di adeguatezza della tutela dei dati personali dei paesi terzi, Consultabile su:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

Commissione europea, *Frequently asked questions on the Commission's adequacy finding on the Canadian Personal Information Protection and Electronic Documents Act,* Consultabile su:
http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/third-countries-faq/index_en.htm

Comunicato stampa della Commissione Europea del 2 febbraio 2016, Consultabile su
http://europa.eu/rapid/press-release_IP-16-216_it.htm

U.S. Department of Homeland Security, U.S. Customs and Border Protection Passenger Name Record (PNR) Privacy Policy, Consultabile su:
https://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf

Edward Hasbrouck, *What's in a Passenger Name Record (PNR)?* Consultabile su:
http://hasbrouck.org/articles/PNR.html

Comunicazione della Commissione al Consiglio e al Parlamento europeo - Trasferimento di dati di identificazione delle pratiche (PNR): un approccio globale dell'UE Consultabile su: http://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A52003DC0826

Ansa, 27 marzo 2012, *Terrorismo: Pe cede a Usa,ok a trasferimento dati passeggeri*, Consultabile su:http://www.ansa.it/europa/notizie/rubriche/altrenews/2012/03/27/visualizza_new.html_157702446.html

Comunicati stampa del Parlamento europeo, 19 aprile 2012, "*Il Parlamento dà il via libera all'accordo con gli USA sui dati dei passeggeri aerei*, Consultabile su:
http://www.europarl.europa.eu/news/it/news-room/20120419IPR43404/il-pe-d%C3%A0-il-via-libera-all'accordo-con-gli-usa-sui-dati-dei-passeggeri-aerei

European digital rights, *Is the new EU-US PNR Agreement acceptable?* , Consultabile su:
https://edri.org/files/2012EDRi_US_PNRcomments.pdf

Conferenza stampa del Parlamento europeo, 24 aprile 2013 "Civil Liberties Committee rejects EU Passenger Name Record proposal" Consultabile su: http://www.europarl.europa.eu/news/en/news-room/20130422IPR07523/civil-liberties-committee-rejects-eu-passenger-name-record-proposal

Riunione straordinaria del Consiglio d'Europa del 30 agosto 2014 Consultabile su:
http://www.consilium.europa.eu/en/meetings/european-council/2014/08/30/

Attentato alla sede di Charlie Hebdo Connsultabile su:
https://it.wikipedia.org/wiki/Attentato_alla_sede_di_Charlie_Hebdo

Riunione informale dei capi di Stato a Brussels il 12 febbraio 2015 Consultabile su:
http://www.consilium.europa.eu/en/press/press-releases/2015/02/150212-european-council-statement-fight-against-terrorism/

Consiglio europeo, Disciplina dell'uso dei dati del codice di prenotazione (PNR) Consultabile su:
http://www.consilium.europa.eu/it/policies/fight-against-terrorism/passenger-name-record/

Intervista dell'ANSA al Garante europeo della protezione dei dati Giovanni Buttarelli del 14 aprile 2016, Consultabile su: http://www.ansa.it/europa/notizie/rubriche/altrenews/2016/04/14/garante-privacy-ue-pnr-e-infortunio-normativo_d9014be4-028e-477a-9479-18cc06f72d51.html

Conclusioni dell'avvocato generale Paolo Mengozzi sulla domanda di parere 1/15 Consultabile su:
http://curia.europa.eu/juris/document/document.jsf?text=&docid=183140&pageIndex=0&doclang=it&mode=req&dir=&occ=first&part=1#Footref105

SWIFT, About Us https://www.swift.com/about-us

Lichtblau & Risen, 23 giugno 2006 '*Bank Data is Sifted by US in Secret to Block Terror', New York Times*, Consultabile su: http://www.nytimes.com/2006/06/23/washington/23intel.html

Discorso di Jean-Claude Trichet, Presidente della BCE al Parlamento europeo del 4 ottobre 2006. Consultabile su: https://www.ecb.europa.eu/press/key/date/2006/html/sp061004.en.html

Comunicato stampa del Parlamento europeo, 10 febbraio 2016, SWIFT: il Parlamento europeo boccia l'accordo con gli USA. Consultabile su:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20100209IPR68674+0+DOC+XML+V0//IT

Comunicati stampa del Parlamento europeo, 16 novembre 2011, SWIFT implementation report: MEPs raise serious data protection concerns, Consultabile su:
http://www.europarl.europa.eu/news/en/news-room/20110314IPR15463/swift-implementation-report-meps-raise-serious-data-protection-concerns

Legislazione:

Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali

Convenzione n.108 sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale

Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati

Regolamento 45/2001/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte

delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati. In vigore dal 1 febbraio 2001

Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche

Carta dei diritti fondamentali dell'Unione europea

Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati

USA Freedom Act, USA Patriot Act e Digital Millennium Copyright Act (DMCA)

Convenzione di Berna per la protezione delle opere letterarie e artistiche

2000/518/CE: Decisione della Commissione, del 26 luglio 2000, riguardante l'adeguatezza della protezione dei dati personali in Svizzera a norma della direttiva 95/46/CE

Opinion No 5/99 on The level of protection of personal data in Switzerland

2002/2/CE: Decisione della Commissione, del 20 dicembre 2001, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della protezione fornita dalla legge canadese sulla tutela delle informazioni personali e sui documenti elettronici (Canadian Personal Information Protection and Electronic Documents Act)

Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act

2003/490/CE: Decisione della Commissione, del 30 giugno 2003, conforme alla direttiva 95/46/CE del Parlamento europeo e del Consiglio e riguardante l'adeguatezza della tutela dei dati personali fornita in Argentina

Opinion 4/2002 on the level of protection of personal data in Argentina

2000/520/CE: Decisione della Commissione, del 26 luglio 2000, a norma della direttiva 95/46/CE del Parlamento europeo e del Consiglio sull'adeguatezza della protezione offerta dai principi di approdo sicuro e dalle relative «Domande più frequenti» (FAQ) in materia di riservatezza pubblicate dal Dipartimento del commercio degli Stati Uniti.

Parere 01/2016 WP238 sulla decisione di adeguatezza della bozza di accordo “Privacy Shield EU-US”

Convenzione sull'aviazione civile internazionale

Parere 4/2003 sul livello di protezione assicurato negli Stati Uniti per quanto riguarda la trasmissione di dati relativi ai passeggeri del 13 giugno 2003 - WP 78

Parere 2/2004 sul livello di protezione adeguato dei dati a carattere personale contenuti nelle pratiche Passeggeri (PNR –Passenger Name Record) trasferite all'Ufficio delle dogane e della protezione di frontiera degli Stati Uniti (Bureau of Customs and Border Protection - US CBP) del 29 gennaio 2004 - WP 8

Decisione della Commissione del 14 maggio 2004 relativa al livello di protezione adeguato dei dati personali contenuti nelle schede nominative dei passeggeri aerei trasferiti all'Ufficio delle dogane e della protezione delle frontiere degli Stati Uniti United States' Bureau of Customs and Border Protection

Decisione del Consiglio del 17 maggio 2004 relativa alla conclusione di un accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (Passenger Name Record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti

Accordo tra la Comunità europea e gli Stati Uniti d'America sul trattamento e trasferimento dei dati di identificazione delle pratiche (passenger name record, PNR) da parte dei vettori aerei all'ufficio doganale e di protezione dei confini del dipartimento per la sicurezza interna degli Stati Uniti

Parere 10/2011 sulla proposta di direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi adottato il 5 aprile 2011

Parere del Garante europeo della protezione dei dati sulla proposta di una direttiva del Parlamento europeo e del Consiglio sull'uso dei dati del codice di prenotazione (Passenger Name Record, PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e dei reati gravi

Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE

Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)

Decisione 2010/16/PESC/GAI del Consiglio del 30 novembre 2009 relativa alla firma, a nome dell'Unione europea, dell'accordo tra l'Unione europea e gli Stati Uniti d'America sul trattamento e il trasferimento di dati di messaggistica finanziaria dall'Unione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi

Parere del Garante europeo della protezione dei dati 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'U nione europea agli Stati Uniti ai fini del programma di controllo delle transazioni finanziarie dei terroristi (TFTP II)

Giurisprudenza:

Corte Suprema degli USA, New York Times Co. vs Sullivan, decisione del 9 marzo 1964 della

Sentenza della Corte (Grande Sezione) 13 maggio 2014, Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos (AEPD), Mario Costeja González

Decisione del comitato ristretto del CNIL del 10 marzo 2016 n.2016-054

Tribunale di Roma, sez. I Civile, sentenza 24 novembre – 3 dicembre 2015, n. 23771

Cour de cassation de Belgique, 29 aprile 2016, N° C.15.0052.F Le Soir contre Oliver G.

Provvedimenti a seguito di richieste di cancellazione, dai risultati resi da un motore di ricerca, dei collegamenti alle pagine web che contengono il nominativo dell'interessato - 6 novembre 2014

Provvedimenti a seguito di richieste di cancellazione, dai risultati resi da un motore di ricerca, dei collegamenti alle pagine web che contengono il nominativo dell'interessato - 11 dicembre 2014

Corte di giustizia, Causa Maximillian Schrems contro Data Protection Commissioner (Schrems), C-362/14, ECLI:EU: C:2015:650 del 6 ottobre 2015

Corte di giustizia, Cause riunite C-317/04 e C-318/04 Parlamento europeo contro Consiglio dell'Unione europea e Commissione delle Comunità europee

Corte di giustizia, Cause riunite C-293/12 e C-594/12 Digital Rights Ireland e Seitlinger e a.