UNIVERSITÀ DEGLI STUDI DI MILANO

DIPARTIMENTO
Dipartimento di diritto pubblico italiano e sovranazionale

CURRICULUM / CORSO DI DOTTORATO
Dottorato in diritto pubblico, internazionale ed europeo
XXXI ciclo

TESI DI DOTTORATO DI RICERCA

LIMITAZIONI E DEROGHE ALLA TUTELA DEI DATI PERSONALI PER RAGIONI DI SICUREZZA NAZIONALE ED ESIGENZE DI LAW ENFORCEMENT NEL DIRITTO INTERNAZIONALE E NEL DIRITTO DELL'UNIONE EUROPEA

IUS 13

Elena Kaiser
Matricola n. 11180

TUTOR
Chiar.ma Prof.ssa Ilaria Viarengo

COORDINATORE DEL DOTTORATO
Chiar.ma Prof.ssa Diana Urania Galetta

A.A.
2017-2018

A mio padre,

RINGRAZIAMENTI

La stesura di questo elaborato costituisce il frutto di un lavoro durato quasi tre anni, trascorso in parte all'Università di Milano e in parte all'estero, principalmente ad Amsterdam nei Paesi Bassi.

Questo lavoro non sarebbe stato possibile grazie al supporto del mio tutor, la Professoressa Ilaria Viarengo, che ha sempre appoggiato ogni mia richiesta e mostrato estrema disponibilità e comprensione, nonché al mio co-tutor, il Professor Marco Pedrazzi. Ringrazio anche il mio "professore genovese" Francesco Munari, per avere sempre creduto in me.

Un ringraziamento particolare va anche alle mie due colleghe Lenka e Beatrice, con cui ho intrapreso tre anni fa questo percorso.

I mesi trascorsi all'estero sono state per me esperienze estremamente ricche sia dal punto di vista culturale, intellettuale, che umano. Ringrazio quindi innanzitutto il Max Planck Institute for Comparative Public Law and International Law di Heidelberg, per la disponibilità del personale bibliotecario, nonché l'ambiente vibrante e pieno di giovani ricercatori con cui ho avuto la fortuna di condividere tre mesi di ricerca. Un grazie particolare va a Valentina, Erendira, Armando e Lorenzo: che possano questi anni essere solo l'inizio di un'amicizia duratura.

Il mio grazie più sincero va anche all'Institute for Information Law, i miei ultimi mesi trascorsi ad Amsterdam sono stati fondamentali per la stesura finale dell'elaborato e di questo ringrazio in particolar modo il direttore dell'Istituto, il professore Nico van Eijk, e la Professoressa Kristina Irion. Le lunghe discussioni e i confronti con tutti i ricercatori dell'Istituto hanno certamente contribuito arricchirmi e a rendere questi mesi indimenticabili. Di questo ringrazio il mio compagno di stanza, Ronan, nonché Max, Sarah, Joao, Valeria, Elena, Begona, Paddy, Gijs e tutti gli altri giovani "iviriani".

Infine, ringrazio i miei genitori e la mia famiglia, per avermi supportato in questo lungo percorso, nonché le mie care amiche Camilla, Elena, Martina, Alice, Chiara, Giulia, Alessandra, Alessandra, Iole e Susi. Il loro supporto ed appoggio emotivo dimostratomi anche durante i mesi di lontananza sono stati per me fondamentali.

INDICE

CAPITOLO 1
IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI NEL DIRITTO INTERNAZIONALE E LE CLAUSOLE DI LIMITAZIONE

1.1 INTRODUZIONE E OGGETTO DI INDAGINE

L'attacco terroristico dell'11 settembre ha segnato senz'altro un punto di svolta nel contesto internazionale. A livello giuridico, ad esempio, a partire da quel momento un buon numero di politici, accademici e studiosi del diritto hanno iniziato ad interrogarsi – senza giungere tuttora ad una soluzione – circa il bisogno di trovare un "giusto bilanciamento" fra la tutela dei diritti umani e le esigenze di sicurezza nazionale, tra cui rientra anche il contrasto al fenomeno terroristico internazionale. Invero, alcuni diritti, che sembravano ormai consolidati in un contesto in internazionale che aveva vissuto anni di relativa tranquillità politica, venivano messi in forte discussione e, improvvisamente, veniva avvertita come eccessiva la libertà di espressione, la privacy e gli altri diritti individuali, che dovevano essere quindi limitati in un contesto sempre più minacciato dal terrorismo internazionale.

Al fine di contrastare il suddetto fenomeno, i singoli Stati e, in alcuni casi, l'intera comunità internazionale, hanno adottato nel corso degli ultimi anni diverse misure di sicurezza e di repressione - le quali, nate per fare fronte ad un'emergenza contingente e limitate nel tempo, sono diventate nella maggior parte dei casi permanenti[1]. Si pensi, ad esempio, agli interrogatori "rinforzati", all'espulsione di soggetti non desiderati, alla creazione di nuovi reati quali il finanziamento di movimenti terroristici e, infine, all'introduzione di nuove tecniche di sorveglianza di massa attraverso il controllo della corrispondenza, delle comunicazioni elettroniche e degli spostamenti spaziali degli individui.

La presente ricerca si ispira e fa riferimento al presente dibattito e si prefigge l'obiettivo di analizzare le limitazioni /deroghe apposte al diritto alla protezione dei dati

[1]Ad esempio, l'*USA Patriot Act* del 2001, adottato dal Congresso statunitense all'indomani dell'attacco terroristico alle Torri gemelle e fortemente limitativo della libertà e dei diritti dei cittadini americani, era destinato a trovare attuazione solo fino al 31 dicembre 2005 ma è stato, poi, "normalizzato" e riautorizzato rendendo di fatto stabili 14 delle 16 disposizioni che erano in scadenza. Cfr. M. SIMONCINI, *Risk Regulation Approach to EU Policy against Terrorism in the light of the ECJ/CFI jurisprudence*, in *German Law Journal* 2009, pag. 529 e ss.

personali anche alla luce dei recenti sviluppi legislativi e giurisprudenziali, resi soprattutto nel contesto legislativo dell'Unione europea e del Consiglio d'Europa.

Il tema della protezione della privacy è tornato in primo piano soprattutto in seguito alle rivelazioni di Snowden nel 2013, ove erano state rese pubbliche informazioni sui programmi di sorveglianza di massa dei cittadini statunitensi e non - operati dall'agenzia di sicurezza nazionale (NSA) e resi possibili anche grazie alla collaborazione delle principali aziende private che gestivano servizi di comunicazioni *online* – che si erano concretizzati nella raccolta indiscriminata di dati personali[2]. Orbene, dal punto di vista strettamente giuridico, i suddetti accordi erano però illegali, in quanto lo Stato avrebbero dovuto ricorrere a strumenti di diritto pubblico, a leggi pubbliche, per controllare i propri cittadini, e non invece, come era avvenuto nel caso di specie, a contratti di diritto privato.

Il cosiddetto *Data Gate* ha destato forte sconcerto nell'opinione pubblica, poiché si è acquisita per la prima volta consapevolezza dell'eventualità che individuo, in maniera del tutto ingiustificata e indiscriminata, potesse essere oggetto di misure di sorveglianza da parte delle pubbliche autorità. La raccolta di dati personali avveniva infatti su larga scala, in maniera automatizzata e segreta– ricorrendo ai cosiddetti *big data.* L'acquisizione delle informazioni avveniva principalmente tramite due modalità, ossia l'intercettazione diretta del flusso di informazioni (programma UPSTREAM) e l'accesso ai dati degli utenti conservati nelle banche dati dei principali servizi di telecomunicazione di società con sede negli stati Uniti (programma PRISM).

Le rivelazioni di Snowden hanno, non dimeno, interferito sui delicati equilibri statali, nella misura in cui è le informazioni personali raccolte riguardavano anche i capi di Stato e di governo[3], e hanno evidenziato come la digitalizzazione delle comunicazioni abbia

[2]L'NSA era riuscita a raccogliere i dati sia stipulando contratti di diritto privato soprattutto con Google, sia entrando direttamente nel network della società. Occorre, infatti, sottolineare che all'epoca dei fatti, diversamente da quanto accade oggi, le informazioni non venivano ancora criptate. La criptazione delle informazioni ha fatto sì che ora le società di *hackeraggio* siano più interessate ad entrare nell'intero *device*. Sul tema la dottrina è molto ampia, solo per citare alcuni contributi cfr. Y. RONEN, *Big Brother's Little Helpers: The right to Privacy and the Responsibility of Internet Service Providers,* in *Utrecht Journal of International and European Law*, 2015; N. WITZLEB, D. LINDSAY, M. PATERSON, S. RODRICK, *Emerging Challenges in Privacy Law,* Cambridge Intellectual Property and Information Law, Cambridge 2014, pag. 1 e ss.; I. GEORGIEVA, *The right to privacy under fire – Foreign Surveillance under the NSA and the GCHQ and its compatibility with Art. 17 ICCPR and Art. 8 ECHR,* in *Utrecht Journal of International and European Law* 2015; M. NINO, *Il caso "Datagate": i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti Umani e Diritto Internazionale* 2013, pag. 727 e ss.

[3]Rese possibili grazie al programma dell'agenzia di sicurezza americana denominato PRISM.

facilitato e reso possibile ai governi collezionare una rilevante quantità di informazioni private sui propri cittadini e su gli individui residenti in ogni parte del mondo[4]. Invero, sebbene i dati collezionati nelle comunicazioni non si estendessero ai contenuti delle stesse, essi rivelavano elementi fondamentali della vita delle persone, quali le interazioni con altri, la collocazione spaziale e le abitudini di vita. Tutte queste informazioni potevano essere registrate, immagazzinate, conservate e trasmesse altrove, esponendo così gli individui e le loro vite private ad interferenze senza precedenti.

Ad oggi, la sorveglianza di massa viene concepita dalla maggior parte degli Stati come uno strumento efficace per identificare ed individuare geograficamente i terroristi. Con il termine "sorveglianza delle comunicazioni" si intende infatti ogni attività di monitoraggio, intercettazione, collezione, analisi, uso, accesso, o simili azioni, relative ad informazioni che includono, riflettono o sono generate/relative alle comunicazioni di una persona appartenenti al passato, presente o futuro[5]. Queste misure comportano però notevoli rischi per i diritti degli individui poiché, accanto ai *data base* utilizzati per contrastare la criminalità, ve ne sono numerosi altri, come quelli che monitorano il comportamento dei viaggiatori, le informazioni trasmesse su Internet e in generale attraverso qualsiasi mezzo di telecomunicazione. Tutto ciò fa sì che numerosi dati personali vengano ogni giorno raccolti, collezionati, immagazzinati e poi utilizzati per creare delle connessioni e, in alcuni casi, addirittura influenzare il comportamento delle persone. La gravità del fenomeno rileva nella misura in cui i destinatari di queste misure non sono solo i soggetti effettivamente sospettati di avere commesso dei crimini – la cosiddetta *targeted surveillance* - ma l'intera popolazione.

Lo sviluppo di una "società sorvegliata" è il risultato del convergere di diversi fattori, legati al particolare momento storico che stiamo vivendo. In primo luogo c'è un accresciuto bisogno, sentito sia a livello internazionale sia a quello nazionale, di rinforzare le misure di sicurezza al fine di prevenire attentati da parte di gruppi criminosi e i terroristi internazionali. In secondo luogo, l'applicazione delle suddette misure è stato possibile

[4]Cfr. N. WITZLEB, D. LINDSAY, M. PATERSON, S. RODRICK, *op. cit.,* v. sopra nota 2, pag. 2.
[5]Consiglio per i diritti umani, *Report of the Office of the United Nations High Commissioner for Human Rights*, *The right to privacy in the digital age*, 27esima sessione, 30 giugno 2014, A/HRC/27/37, parr. 3 e 4.

anche grazie al concomitante progresso tecnologico, che ha permesso di immagazzinare e processare un numero sempre maggiore di informazioni personali[6].
A ciò si aggiunga il fatto che la privacy sia ancora classificata dalla dottrina maggioritaria come un diritto individuale, da controbilanciare con altri valori sociali, invece generali, quali la sicurezza nazionale. Entrambi i concetti restano tuttora difficili da definire esaustivamente e, in una società sempre più minacciata dal fenomeno terroristico, la tutela della sicurezza nazionale viene percepita nella maggior parte dei casi come preponderante rispetto alla tutela dei dati personali[7].

Fatte queste premesse, si rende fin da subito opportuno sottolineare che, data l'estensione del tema trattato, nel presente elaborato l'oggetto di indagine verrà circoscritto al diritto alla privacy inteso quale protezione dei dati personali, con particolare attenzione alle limitazioni che esso può subire per esigenze di *law enforcement* e di tutela della sicurezza nazionale. Inoltre, il tema della protezione dei dati personali presuppone una conoscenza, seppur basilare, di alcune concetti informatici quali la crittografia e anonimizzazione. A ciò si aggiunga il fatto che altri concetti, come la privacy e la sicurezza nazionale, siano tuttora vaghi e di difficile definizione. Alla luce di queste considerazioni, di fondamentale importanza appaiono alcune precisazioni di natura terminologia, nei limiti peraltro dell'oggetto della presente indagine e delle necessariamente limitate conoscenze tecniche di alcuni strumenti propri di contesti tecnici diversi da quello giuridico. Si procederà pertanto a differenziare, innanzitutto, i concetti di sicurezza nazionale, sicurezza pubblica e ordine pubblico e poi a definire, nel corso del quinto capitolo, le tecniche della crittografia e dell'anonimizzazione.

In primo luogo, occorre distinguere fra sicurezza nazionale, *law enforcement* e ordine pubblico, sulla base della dottrina italiana. La distinzione risulta infatti di fondamentale importanza, determinando quale legge è applicabile al singolo caso.

La sicurezza nazionale è un concetto molto ampio, ad oggi non ancora esaustivamente definito, che ricomprende al suo interno diversi significati. Infatti, nonostante tale nozione sia comunemente richiamata, specialmente quale limite

[6]Cfr. M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection,* in *Vienna Online Journal on International Constitutional Law* 2010, pag. 409.
[7]Cfr. M. H. MURPHY*, Surveillance and the Right to Privacy: Is an "Effective Remedy" possible?, in Justiciability of Human Rights Law in Domestic Jurisdictions*, Edited by A. DIVER and J. MILLER, Springer, Svizzera 2016, pag. 289.

all'applicazione dei diritti umani, dagli organi e dalle corti internazionali – quale la Corte europea dei diritti umani nei noti casi *Roman Zakharov c. Russia*[8] *e Zsabo e Vissy c. Ungheria*[9] – definirne il suo esatto contenuto e, soprattutto, il suo ambito di applicazione, rimane prerogativa dei singoli Stati, i quali lo modellano ed estendono a seconda delle contingenze del momento. Invero, come si vedrà nel proseguio del presente lavoro, neanche la Corte europea dei diritti umani sembra venire in aiuto per risolvere i dubbi che persistono circa l'ambito di applicazione delle clausole di limitazione fondate su ragioni di sicurezza nazionale, ricorrendo spesso, in maniera indistinta ed interscambiabile, ai termini di sicurezza nazionale e di *law enforcement.*

Per quanto riguarda, ad esempio, l'ordinamento giuridico italiano, la Corte Costituzionale definisce la "[…] sicurezza dello Stato nella sua personalità internazionale – riconosciuto dall'art. 52, in correlazione agli artt. 1 e 5 Cost. – vale a dire l'interesse dello Stato-comunità alla propria integrità territoriale e alla propria indipendenza, coincidente, al limite, con la sopravvivenza dello Stato stesso […]"[10]. Occorre inoltre evidenziare come alla tradizionale accezione "oggettiva" di sicurezza nazionale, se ne sia recentemente affiancata una di tipo "soggettivo", in base alla quale la sicurezza potrebbe configurarsi anche come un diritto individuale e soggettivo, ossia come un diritto facente capo ad ogni cittadino di sentirsi tutelato da parte del proprio Stato contro le eventuali minacce interne ed esterne[11].

A livello legislativo europeo, la prerogativa statale in materia di sicurezza nazionale è riconosciuta espressamente dall'articolo. 4, par. 2, TUE[12], ai sensi del quale "L'Unione rispetta […] le funzioni essenziali dello Stato, in particolare le funzioni di salvaguardia dell'integrità territoriale, di mantenimento dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro". Secondo l'interpretazione fornita alla norma dalla Corte di giustizia, nella nozione di sicurezza nazionale viene ricompresa "[…] sia la sicurezza interna che quella

[8]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, sentenza del 4 dicembre 2015, ricorso n. 47143/06.
[9]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria*, sentenza del 12 gennaio 2016, ricorso n. 37138/14.
[10]Corte Costituzionale, sentenza del 23 febbraio 2012, n. 40.
[11]Cfr. L. LORELLO, *Il dilemma sicurezza vs. libertà al tempo del terrorismo*, in *Democrazia e Sicurezza – Democracy and Security Review* 2017, pag. 6.
[12]Lo stesso principio viene inoltre ribadito sia dall'articolo 2, par. 2, regolamento (UE) 2016/679 sia dall'articolo 2, par. 3, direttiva (UE) 2016/680.

esterna di uno Stato membro, e quindi la presenza del rischio di un pregiudizio al funzionamento delle istituzioni e dei servizi pubblici essenziali, nonché alla sopravvivenza della popolazione, oppure anche del rischio di perturbazioni gravi dei rapporti internazionali o degli interessi militari"[13].

L'ordine pubblico può essere suddiviso, invece, in ordine pubblico "ideale", ossia l'insieme di principi ispiratori e legittimanti le attività di polizia di prevenzione e tutela, come limite immanente a tutte le libertà civili e politiche, e ordine pubblico "materiale", ossia l'insieme di beni specifici oggetto di tutela[14]. Strettamente funzionale al mantenimento dell'ordine pubblico è la pubblica sicurezza, che trova ad esempio in Italia la sua specifica disciplina nel Testo Unico Leggi Pubblica Sicurezza, approvato con Regio Decreto del 18 giugno 1931. In particolare, l'art.1 dispone che "L'autorità di pubblica sicurezza veglia al mantenimento dell'ordine pubblico, alla sicurezza dei cittadini, alla loro incolumità ed alla tutela della proprietà; cura l'osservanza delle leggi e dei regolamenti generali e speciali dello Stato, delle province e dei Comuni, nonché delle ordinanze delle autorità; presta soccorso nel caso di pubblici e privati infortuni […]".

Infine, l'attività di *law enforcement* è generalmente definita come "[…] the operation of all that body of procedural machinery by which the substantive or positive law is enforced […]"[15]. Inoltre, con riferimento all'ordinamento europeo, per "autorità di law enforcement" - traducibile in italiano come "autorità preposte all'applicazione della legge" – s'intendono generalmente gli organismi di polizia e giudiziari, nonché quelli che eseguono controlli alle frontiere esterne degli Stati ovvero controlli di dogana[16], che hanno il compito di "individuare, prevenire e indagare i reati o le attività criminali, esercitare l'autorità e adottare misure coercitive nell'ambito di tali funzioni". Diversamente da quanto previsto in materia di sicurezza nazionale, l'Unione europea ha competenza concorrente con quella degli Stati membri nel legiferare nel campo della *law enforcement* che fa parte, in seguito al Trattato di Lisbona, dello spazio di sicurezza, libertà e giustizia[17]. Sempre

[13]Corte di giustizia (Grande Sezione), *J.N. c. Staatssecretaris van Veiligheid en Justitie*, 15 febbraio 2016, C-443/14 e 444/14, par. 66.
[14]Cfr. F. PAOLOZZI, *Focus sulla giurisprudenza costituzionale in materia di pubblica sicurezza*, in *Osservatorio Regionale* 2011, pag. 887.
[15]J. C. HUTCHESON, *Law enforcement*, in *Central Law Journal* 1922, pag. 393.
[16]Con particolare riferimento all'ordinamento europeo, cfr. art. 2 (a), della Decisione Quadro 2006/960/GAI, in GUUE L 386, 29.12.06, pp. 89–100.
[17]L'articolo 3, par. 2, TUE prevede, infatti, che "L'Unione offre ai suoi cittadini uno spazio di libertà, sicurezza e giustizia senza frontiere interne, in cui sia assicurata la libera circolazione delle persone insieme a

grazie al Trattato di Lisbona e all'abolizione dei tre pilastri[18], le decisioni in questo settore vengono adottate tramite procedura legislativa ordinaria e sono soggette al metodo comunitario[19].

In merito occorre inoltre sottolineare come il concetto di *law enforcement* negli Stati Uniti sia più ampio e ricomprenda "prevention, detection, suppression, investigation, or prosecution of any criminal offense or violation of law related to border enforcement, public security, and national security, as well as for non-criminal judicial or administrative proceedings related directly to such offenses or violations"[20]. Questa concezione più ampia ha rilevato nella misura in cui i programmi di sorveglianza di massa precedentemente citati fossero considerati per la legge americana conformi alla legge e in contrasto, invece, con la normativa europea[21].

Per quel che interessa il presente oggetto di indagine, il 4 maggio 2016 è stata pubblicata la direttiva che regola i trattamenti dei dati personali nei settori di prevenzione, contrasto e repressione dei crimini (direttiva (UE) 2016/680), che abroga la precedente decisione quadro 2008/977/GAI del Consiglio. La direttiva è divenuta necessaria in ragione dell'importanza fondamentale che lo scambio di informazioni, e quindi anche dei dati, ha assunto all'interno delle diverse politiche dell'Unione europea e, soprattutto, in un settore così delicato come la cooperazione giudiziaria e di polizia in materia penale[22].

---

misure appropriate per quanto concerne i controlli alle frontiere esterne, l'asilo, l'immigrazione, la prevenzione della criminalità e la lotta contro quest'ultima". Cfr. in dottrina F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice,* Springer Heidelberg, Dordrecht London New York 2012, pag. 6 e ss.

[18]Prima del Trattato di Lisbona, questo settore rientrava nel terzo pilastro, ossia nella "Cooperazione di polizia e giudiziaria in materia penale" (GAI).

[19]Il metodo comunitario, che è divenuto a partire dal Trattato di Lisbona la procedura decisionale ordinaria, è caratterizzato dall'interazione tra la Commissione europea, il Parlamento europeo e il Consiglio dei Ministri. Esso si differenzia, invece, dall'altro metodo, quello intergovernativo, in cui gli Stati membri condividono con la Commissione il diritto di iniziativa.

[20]R.Z. GEORGE, H. RISHIKOF, *National Security Enterprise:Navigating the Labyrinth*, Georgetown University Press 2017, pag. 288. Cfr. anche E. DE BUSSER, *EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?,* in *Utrecht Law Review* 2010, pag. 97. Articolo 5, par. 1, *U.S.-Europol Supplemental Agreement on the Exchange of Personal Data and Related Information* (December 20, 2002), disponibile alla pagina https://www.state.gov/s/l/38629.htm.

[21]*Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 23 novembre 2009, doc. n. 15851/09 JAI 822 DATAPROTECT 74 USA 102, pagg. 3 e 4.

[22]Le principali agenzie europee che operano in questo settore sono: Europol, Frontex, OLAF (Commissione antifrode), Customs Information System (CIS), Schengen Information System (SIS), Visa Information System (VIS).

1.2 LIMITAZIONE DELL'OGGETTO DI INDAGINE

Sotto un profilo strettamente geografico, il presente lavoro riguarda principalmente il contesto europeo, come, cioè, il problema della protezione dei dati personali sia stato affrontato dai principali organi giurisdizionali europei. Il riferimento è soprattutto alla recente giurisprudenza della Corte europea dei diritti umani - la quale ha sancito nei casi *Roman Zakharov c. Russia*[23] e *Szabo e Vissy c. Ungheria*[24] gli standard minimi europei in materia di sorveglianza di massa – e a quella della Corte di giustizia che , con le sentenze *Digital Rights Ireland*[25] e *Maximilian Schrems*[26], ha invalidato, rispettivamente, la direttiva 2006/24/CE e il cosiddetto pacchetto "Safe Harbour".

Meritano inoltre di essere ricordate altre due pronunce, ancora più recenti, della Corte europea dei diritti umani, *Centrum of Rattvisa c. Svezia*[27] e *Big Brother Watch e altri c. Regno Unito*[28], riguardanti i sistemi di sorveglianza di massa posti in essere rispettivamente in Svezia e nel Regno Unito.

La scelta di escludere dal presente elaborato la disciplina normativa e la giurisprudenza relativa al diritto alla privacy nel sistema statunitense si giustifica in ragione delle profonde differenze sostanziali che intercorrono fra i due approcci, che costituirebbero, da soli, oggetto di due differenti e autonome trattazioni. Basti pensare, ad esempio, che mentre nella visione "europea" il diritto alla privacy viene concepito come un diritto fondamentale facente capo all'individuo, in quella americana esso costituisce un diritto strettamente legato al consumatore tutelato dalla *Federal Trade Commission* e che deve essere, quindi, controbilanciato con le diverse esigenze economiche delle imprese.
Le profonde differenze intercorrenti fra le due concezioni di privacy derivano dal diverso contesto politico in cui si sono rispettivamente originate, che ha condotto, rispettivamente,

[23]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit.
[24]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria*, cit.
[25]Corte di giustizia dell'Unione europea (Grande Sezione), *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung* e altri, sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12.
[26]Corte di giustizia dell'Unione europea (Grande Sezione) *Maximilian Schrems c. Data Protection Commissioner, con l'intervento di Digital Rights Ireland Ltd*, sentenza del 6 ottobre 2015, C-362/14 e C-362/14.
[27]Corte europea dei diritti umani, *Centrum För Rättvisa c. Svezia*, sentenza del 19 giugno 2018, ricorso n. 35252/08.
[28]Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito*, sentenza del 13 settembre 2018, ricorsi nn. 58170/13 e altri.

ad una diversa percezione dell'elemento di esterno di minaccia. Invero, nella concezione statunitense la privacy viene originariamente intesa come "libertà" da qualsiasi intrusione statale e, conseguentemente, viene percepita come minaccia ogni intrusione della forza pubblica nel proprio domicilio o nella propria corrispondenza. La privacy è, inoltre, strettamente connessa ai concetti di controllo e alla possibilità di scelta. Nella concezione europea, invece, la privacy è collegata al concetto di "dignità" e, essendo un diritto fondamentale dell'individuo, è compito dello Stato proteggerlo.

A livello legislativo, il diritto al rispetto della vita privata è stato inserito dal *Bill of Rights* nel 1871, il quale ha previsto al IV emendamento alla Costituzione americana che "Non sarà violato il diritto dei cittadini di godere della sicurezza personale, della loro casa, delle loro carte e dei loro beni, di fronte a perquisizioni e sequestri ingiustificati; e non si rilasceranno mandati di perquisizione se non per motivi sostenuti da giuramento o da dichiarazione solenne e con descrizione precisa del luogo da perquisire e delle persone da arrestare o delle cose da sequestrare". Il diritto in questione, pur costituendo un principio costituzionale, viene disciplinato in maniera molto frammentaria dalle diverse leggi settoriali – non esistendo ad oggi una legge generale federale ad ampia portata, a parte il *Privacy Act* del 1974 – e questo lo rende molto più vulnerabile alle contingenze politiche, che richiedono di volta in volta di limitarlo. La tutela della privacy nel sistema giuridico americano ha mostrato tutta la sua vulnerabilità dopo gli attacchi terroristici alle Torri Gemelle, quando il governo federale ha emanato una serie di misure restrittive dei diritti fondamentali degli individui, senza che fossero fornite le opportune garanzie contro eventuali abusi statali[29].

La stessa Corte di giustizia dell'Unione europea ha inoltre recentemente evidenziato, seppur in maniera indiretta come si avrà modo di analizzare in seguito nel noto caso *Maximilian Schrems c. Data Protection Commissioner*[30], come il livello di tutela offerto oltreoceano in materia di dati personali non sia sufficientemente adeguato e conforme agli standard previsti dalla Carta dei diritti fondamentali dell'Unione europea e dalla direttiva

[29]Si fa riferimento, soprattutto, al *Patrioct Act* (Legge 107-56 del 26 ottobre 2001) promulgato all'indomani dell'11 settembre. Esso, dopo diverse proroghe, è stato finalmente sostituito durante la presidenza Obama dal Freedom Act (Giugno 2015), che ha apposto delle limitazioni al controllo sistematico dei dati telefonici, dal momento che era stato dimostrato più volte che non erano stati così determinanti al fine di prevenire gli attacchi terroristici. Per quanto riguarda le tutele riconosciute ai cittadini non americani, le differenze rispetto al *Patrioct Act* sono minimali.

[30]Corte di giustizia (Grande Sezione), *Maximilian Schrems,* cit.

95/46/CE in materia di dati personali. Questa diversità esporrebbe però a gravi rischi anche i dati personali relativi ai cittadini europei, che potrebbero venire trasmessi e trattati in Paesi terzi, dove la tutela della privacy nei confronti degli stranieri a volte è pressoché nulla. Basti solo pensare che negli Stati Uniti viene fatta una netta distinzione, a livello legislativo, fra i diritti spettanti ai cittadini americani e ai non americani, negando di fatto il riconoscimento della privacy a questi ultimi[31]. A tal proposito, una delle più grande sfide che dovranno affrontare le Autorità garanti privacy nazionali e il Garante europeo dei dati personali in relazione al nuovo regolamento (UE) 2016/679 sarà quella di garantire una tutela effettiva dei dati personali europei anche nel caso in questi siano processati da società stabilite in Paesi terzi, ma che offrono beni o servizi, o monitorano i comportamenti, degli interessati che si trovano nell'Unione europea (articolo 3).

[31]Il Privacy Act (The Privacy Act of 1974,5 U.S.C. §552° (2012), ossia la legge statunitense che disciplina la raccolta, il trattamento e la diffusione dei dati personali da parte delle agenzie federali, differenzia tra i cittadini statutnitensi – cui sono equiparati gli "alien[s] lawfully admitted for permanent residence" – e i cittadini stranieri, garantendo a quest'ultimi minori tutele. In dottrina cfr. D. SEVERSON, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, in *Harvard International Law Journal*, 2015, pagg. 508 e 509.

1.3 METODOLOGIA DELLA RICERCA E STRUTTURA

Per quanto riguarda la metodologia, il punto di partenza, nonché il nucleo centrale dell'oggetto di indagine del presente elaborato, vuole essere l'analisi critica della recente giurisprudenza in materia di diritti umani con riguardo alla protezione dei dati personali. Questa scelta si giustifica per un duplice motivo: innanzitutto, emerge in maniera evidente la poca chiarezza, nonché la brevità, dei contenuti delle fonti internazionali che proteggono i dati personali, le quali esauriscono in pochi paragrafi la descrizione della disciplina e le limitazioni al suddetto diritto. Si è reso pertanto necessario, soprattutto per quanto concerne l'articolo 8 CEDU, un sistematico ed analitico lavoro di interpretazione giurisprudenziale da parte dei giudici di Strasburgo al fine delimitare, ma soprattutto chiarire, il contenuto del diritto alla privacy e alla protezione dei dati personali.

Il secondo motivo, strettamente interconnesso al primo, riguarda l'importanza dei principi sanciti recentemente dalla Corte di giustizia dell'Unione europea e dalla Corte europea dei diritti umani, che hanno influenzato anche la successiva adozione degli strumenti normativi in materia di protezione dei dati personali. A ciò si aggiunga inoltre che, in un contesto politico che si sente sempre più minacciato dal fenomeno terroristico e in cui gli Stati tendono ad adottare misure spesso sproporzionate al fine di contrastarlo, le corti nazionali ed internazionali svolgono un ruolo fondamentale nel ridimensionare l'impatto delle leggi nazionali sui diritti fondamentali degli individui, svolgendo un rigido controllo di conformità delle stesse ai principi democratici e alle convenzioni internazionali dei diritti umani[32].

Sempre dal punto di vista metodologico, la ricerca consiste inoltre in un'analisi del diritto internazionale ed europeo attraverso la consultazione di diverse fonti documentali in materia di protezione dei dati personali. Esse consistono nei più importanti strumenti giuridici internazionali – trattati, regolamenti e direttive europee, strumenti di *soft law* – già adottati e, in qualche caso, in fase di adozione, da parte degli Stati membri facenti parte di diverse organizzazioni. Una caratteristica che emerge in maniera sempre più evidente nel contesto della protezione dei dati personali, e già riscontrabile dopo un prima lettura delle fonti normative e giurisprudenziali, è la tendenza a far venire meno le linee di confine tra diritto pubblico e diritto privato. Se è pur vero infatti che, ad oggi, sia il diritto

[32]Cfr. L. LORELLO, *op.cit.*, v. sopra nota 11, pagg. 20 e 21.

internazionale sia il diritto dell'Unione europea – nonché i rispettivi diritti nazionali – differenziano ancora la disciplina applicabile ai dati utilizzati da società private per scopi commerciali da quelli utilizzati, invece, dalle pubbliche autorità per proteggere la sicurezza nazionale, gli istituti utilizzati nell'uno e nell'altro settore presentano sempre più analogie e influenze reciproche. Basti pensare che il nuovo regolamento (UE) 2016/679, pur avendo espressamente escluso dal proprio campo di applicazione l'utilizzo dei dati personali per ragioni di sicurezza nazionale, richiama principi tipici del diritto internazionale dei diritti umani quale quello di proporzionalità e di necessità, i quali non erano presenti invece nella precedente direttiva 95/46/CE. Il venire meno dei confini tra diritto pubblico e diritto privato potrebbe condurre ad una trasformazione del sistema globale in materia di protezione dei dati personali, ossia da un classico sistema di tipo verticale e gerarchico, in cui gli Stati sono i soggetti principali che interagiscono con altri Stati od organizzazioni internazionali, ad uno di tipo orizzontale, in cui le società private e gli enti non governativi partecipano in maniera paritaria ai processi normativi e giurisdizionali globali. La struttura, tipica soprattutto del diritto internazionale commerciale, si fonda sul concetto di "cooperazione" sulla contrattazione privata[33].

1.3.1 Struttura

Dal punto di vista strutturale, l'elaborato analizzerà, innanzitutto, il diritto alla protezione dei dati personali *in abstracto*. In particolare, verrà condotta un'analisi sull'evoluzione del concetto di privacy, dalle origini fino ad oggi, e sulle più rilevanti fonti internazionali ed europee in materia di protezione dei diritti umani.

Dopo avere affrontato le fonti normative, il problema della protezione dei dati personali verrà quindi analizzato in concreto, attraverso un'analisi critica dei più recenti casi giurisprudenziali decisi in materia dalla Corte europea dei diritti umani e dalla Corte di giustizia dell'Unione europea. In particolare, ci si concentrerà sui criteri adottati dai due organi giurisdizionali per stabilire se le legislazioni statali sono conformi all'articolo 8 CEDU e all'articolo 7 della Carta dei diritti fondamentali dell'Unione europea.

[33]La questione del sistema globale come diritto orizzontale, è stata affrontata, con riferimento al diritto amministrativo da M.R. FERRARESE, *Il diritto orizzontale. L'ordinamento giuridico globale secondo Sabino Cassese,* in «Pol. dir.», 2007, pag. 641. Cfr. anche T.L. FRIEDMAN, *Il mondo è piatto. Breve storia del ventunesimo secolo,* Mondadori, Milano 2006, pag. 65.

Infine, verranno identificate e analizzate le principali sfide che dovranno essere affrontare dai sistemi internazionale ed europeo di tutela de diritti umani in materia di protezione dei dati personali nei prossimi anni, soprattutto in relazione allo sviluppo di nuove tecnologie, nonché le possibili soluzioni avanzati dagli Organi internazionali di controllo. La scienza informatica si sviluppa e modifica, infatti, ad una velocità molto più rapida rispetto alla correlata scienza giuridica – dando origine a significativi problemi applicativi dovuti, principalmente, a lacune legislative. Basti pensare, ad esempio, all'utilizzo dei droni da parte degli Stati, per fini non sempre legittimi, oppure ai cosiddetti *cyberattacchi* ad opera di cellule non statali. In entrambi i casi, si generano dei problemi connessi all'esatta collocazione spaziale dei soggetti responsabili e alla possibile all'applicazione extraterritoriale dei trattati sui diritti umani, dal momento che spesso il luogo dove è collocato il *server*, o il computer che manovra i movimenti del drone, si trova in un Paese diverso rispetto a quello in cui si manifestano gli effetti dannosi della condotta illecita.
Ci si soffermerà, in particolare, sul principio di proporzionalità, utilizzato costantemente dagli organi giurisdizionali di Strasburgo e Lussemburgo al fine di soppesare i diversi interessi contrapposti delle parti pubbliche e private nel contesto delle misure di sorveglianza di massa e delle limitazioni ai diritti umani. Il suddetto principio è stato, d'altronde, inserito di recente – unitamente a quello di necessità – nel regolamento (UE) 2016/679, il quale, pur non applicandosi direttamente alle attività riguardanti la sicurezza nazionale, è finalizzato ad uniformare la legislazione degli Stati membri e apporta rilevanti modifiche in materia di tutela dei diritti fondamentali degli individui. Quale ulteriore dimostrazione dell'importanza assunta dal principio di proporzionalità in materia di protezione dei dati personali rilevano il rapporto sul diritto alla privacy adottato nel 2014 dal Consiglio per i diritti umani delle Nazioni Unite[34], nel quale è stata evidenziata la necessità di adottare misure proporzionate al fine di promuovere la democrazia nelle diverse società.

Una particolare attenzione verrà inoltre dedicata al cosiddetto "Data Breach Notification", ossia all'obbligo imposto in capo al titolare del trattamento e al responsabile del trattamento di notificare all'autorità di controllo, e in specifici casi anche all'interessato, la violazione dei dati personali. Questo istituto, originatosi nel contesto

[34]Consiglio per i diritti umani, *Report of the Office of the United Nations High Commissioner for Human Rights*, *The right to privacy in the digital age*, 27esima sessione, 30 giugno 2014, A/HRC/27/37.

giuridico statunitense e ormai adottato anche in diversi Paesi del Sud-est asiatico, è stato ora inserito nel recente regolamento (UE) 2016/679 e nella direttiva (UE) 2016/680 "relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati". Significativo è, soprattutto, l'inserimento del "Data Breach" in quest'ultima fonte legislativa, che riguarda principalmente la tutela dei dati personali nel settore di competenza dell'Unione europea relativa allo spazio di libertà, sicurezza e giustizia, ovvero anche per ragioni di *law enforcement* e potrebbe essere valutata anche un'ulteriore estensione dello stesso al settore della sicurezza nazionale, così come d'altronde recentemente più volte auspicato dalla Corte europea dei diritti umani. Tale estensione permetterebbe una tutela più efficace dei diritti degli individui anche nei confronti degli organi statali e, inoltre, una maggiore regolamentazione a livello normativo arginerebbe il rischio che i dati personali vengano trasmessi a servizi di *intelligence* di Paesi terzi, ove il livello di tutela è inferiore[35]. Occorre, però, rimarcare che ad oggi l'Unione europea, nonostante abbia tentato diverse volte di uniformare le legislazioni dei vari Paesi ed esortato gli stessi ad adottare una definizione comune di sicurezza nazionale, non abbia competenza in materia, che resta prerogativa assoluta degli Stati.

Infine, nel quarto e quindi capitolo verrà posta l'attenzione sulle problematiche tuttora irrisolte nel contesto internazionale ed europeo in materia di tutela dei dati personali e limitazioni per ragioni di sicurezza nazionali ed esigenze di *law enforcement* – in particolare sotto il profilo dell'eventuale imputazione di responsabilità per illecita trasmissione dei dati da parte delle società di diritto privato ed esercizio extraterritoriale della giurisdizione da parte degli organi internazionali di controllo – e sulle possibili proposte avanzate dai suddetti organi per rinforzare il diritto in questione.

[35]Ci si riferisce in particolare agli Stati Uniti, con cui l'Unione europea ha numerosi ed importanti rapporti economici, strategici, militari e di altra natura, e dove è noto, anche in seguito alle rivelazioni di Snowden, che vengono adottati programmi di sorveglianza di massa.

1.4 L'EVOLUZIONE DEL DIRITTO ALLA PRIVACY: DAL *RIGHT TO BE LEFT ALONE* ALLA PROTEZIONE DEI DATI PERSONALI

Dal punto di vista storico, il diritto alla protezione della vita privata e familiare si è originato principalmente a partire dalla fine del XIX secolo nelle società borghesi liberali dei Paesi anglosassoni – i primi ad essere interessati dalla rivoluzione industriale – e si è successivamente espanso anche negli altri ordinamenti liberaldemocratici[36]. Il suddetto diritto risente della concezione liberale secondo cui l'individuo è un soggetto autonomo di diritto, sovrano di se stesso e dotato di una propria dignità[37]. In particolare, la privacy si affianca ad altri diritti fondamentali, quali quello alla vita, all'integrità fisica e mentale e alla personalità giuridica e ha lo scopo di garantire all'individuo non solo la sua esistenza fisica, spirituale e legale ma anche il suo onere e la sua reputazione[38].

Inizialmente, il diritto alla riservatezza era strettamente collegato al rispetto della proprietà privata e non veniva, invece, attribuita alcuna rilevanza all'eventuale danno alla personalità, alla sfera morale. Il concetto di privacy venne coniato per la prima volta nel 1890, quando i due giovani avvocati di Boston Samuel D. Warren e Louis D. Brandeis pubblicarono nella *Harvard Law Review* il famoso articolo "The Right to privacy"[39]. La

[36]Cfr. R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, 2003, pag. 3 e ss. Secondo altri, invece, il dibattito sulla necessità di tutelare la privacy sarebbe sorto nel 1849 nel contesto reale inglese, quando veniva denunciata da parte della Regina Vittoria e di suo marito l'esposizione abusiva da parte di un dipendente di alcuni quadri/incisi ritraenti i loro figli. Questo episodio aveva poi dato origine al noto caso *Principe Albert c. Strange.*

[37]Per una definizione dettagliata della privacy e delle sue sottocategorie cfr. M. NOWAK, *U.N. Covenant on Civil and Political Rights*, CCPR COMMENTARY, N.P. Engel publisher 2005. Cfr. anche C. DOYLE, M. BAGARIC, *The Right to privacy: Appealing, but Flawed,* in I*nternational Journal of Human Rights*, 2005, pag. 52. L'autore ritiene che, in realtà, né il principio di autonomia né quello di dignità siano capaci di fornire un fondamento teorico solido al diritto alla privacy, essendo a loro volta concetti vaghi e relativi.

[38]Cfr. M. NOWAK, *op. cit*., v. sopra nota 37, pag. 378.

[39]Cfr. S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy,* in *Harvard Law Review* 1890. Le motivazioni dietro alla pubblicazione dell'opera sono alquanto singolari. Brandeis, socio di Warren in uno studio legale di Boston, era un uomo di rilevante notorietà all'epoca dei fatti anche grazie al ruolo di giudice che aveva rivestito alla Corte Suprema. Le abitudini mondane della signora Warren, che era solita frequentare locali notturni anche in compagnia di uomini diversi dal marito, erano state oggetto di numerosi articoli di cronaca locale e questo aveva condotto Brandeis a redigere, assieme al collega, l'articolo in questione. In esso veniva analizzato in maniera approfondita e dettagliata il rapporto fra il diritto di cronaca e il rispetto della vita privata, con particolare riferimento al diritto, pressoché illimitato, ad essere informati quando l'individuo era un personaggio di pubblico interesse e, per contro, il diritto assoluto al rispetto della vita privata nel caso in cui i fatti riguardassero un comune cittadino. I due autori differenziavano inoltre il diritto alla privacy dagli altri diritti concernenti la personalità degli individui, quali la proprietà intellettuale e la libertà di espressione. Secondo alcuni autori, però, il diritto alla privacy avrebbe origini ancora più antiche, risalendo, addirittura, all'antica Roma e alle XII Tavole. Sul punto cfr. J.K. WEEKS, *Comparative Law of Privacy*, in *Clev.-Marshall Law Review* 1963, pag. 486 e ss. Secondo un altro filone di pensiero, invece, il diritto alla privacy fonderebbe le sue radici nel diritto ebraico, e in particole nella legge di *Mishnah* risalente al III secolo A.C., che imponeva di rispettare certe regole relative all'altezza delle finestre di edifici contigui,

privacy veniva ivi definita "as the right of an individual to be free from undesired or un unwarranted revelation to the public of matters regarding which the public is not concerned" e come il "right to be left alone"[40]. Il problema di tutelare la vita privata degli individui si era infatti palesato con l'avvento della fotografia e con la possibilità per ciascuno di dotarsi di una propria macchina fotografica. Parallelamente, inoltre, la diffusione dei quotidiani stampati aveva permesso la diffusione di notizie e *gossip* su una scala senza precedenti. In base alla concezione dei due giovani americani, la privacy veniva ora intesa come un diritto all'inviolabilità della personalità", appartenente alla più ampia categoria dei danni morali ("injury of feelings")[41].

Nel corso del XX secolo, grazie all'intervento giurisprudenziale da parte delle corti statunitensi, il diritto ha continuato ad evolversi, venendo prima riconosciuto quale vero e proprio diritto alla personalità – quello che viene tradizionalmente denominato dalla dottrina tedesca come *Persönlichkeitsrech*[42] - e assumendo poi gli attuali connotati della segretezza delle comunicazioni, della protezione generale dei dati personali e del codice genetico degli esseri umani[43]. Il diritto alla privacy ricomprende ad oggi vari sottocategorie di diritti quali: l'identità personale e il nome, il diritto all'immagine, l'integrità, intimità, l'autonomia, la riservatezza delle comunicazioni, la sessualità, il rispetto della famiglia, della casa, della corrispondenza e, infine, dell'onore e reputazione.

---

onde evitare che il vicino potesse guardare dentro la casa dell'altro. Cfr. S.H. HOFSTADTER e G. HOROWITZ, *The right of Privacy,* Central Book Company, New York 1964, pag.9.

[40]Nei decenni successivi, molti altri noti studiosi statunitensi hanno tentato di definire il concetto di privacy. Secondo ROSCOE POUND (1915) e PAUL FREUND (1975), per esempio, la privacy era strettamente connessa alla personalità di un individuo, necessaria per definire la sua essenza quale essere umano. Secondo altri, invece (LOUIS HENKIN), il concetto di privacy riguardava l'autonomia degli individui, la libertà morale di determinarsi nei propri pensieri, azioni e decisioni. Un terzo filone di pensiero, riconducibile principalmente a ALAIN WESTIN e CHARLES, riteneva la privacy un diritto connesso alla capacità degli individui di regolare le informazioni che li riguardavano, le proprie relazioni personali "when, how, and to what extent information about them is communicated to others". Sempre secondo Westin e Charles, nelle società democratiche il diritto perseguiva principalmente quattro funzioni basilari: autonomia personale, il rilascio emozionale, la capacità di autodeterminarsi e, infine, il diritto ad avere una comunicazione riservata e protetta. Vi era, infine, un quarto approccio, misto, che suddivideva la privacy in tre componenti essenziali: "secrecy, anonymity and solitude". Cfr. K. GORMLEY, *One Hundred Years of Privacy*, in *Wiscousin Law Review*, 1992.

[41]Secondo gli americani HARPER E JAMES, la privacy si sarebbe sviluppata come un diritto "parassita", poiché riconosciuta inizialmente dai giudici soltanto in via incidentale quale danno morale connesso al diritto di proprietà, ai diritti derivanti dal contratto o da particolari rapporti di confidenza, quali possono essere, per esempio, quelli che intercorrono fra medico e paziente. Cfr. S.H. HOFSTADTER e G. HOROWITZ, *op. cit.*, v. sopra nota 39, pag.5.

[42]Il momento di svolta si è avuto con il caso *Griswald v. Connecticut* (Corte Suprema degli Stati Uniti d'America, *Griswold c. Connecticut*, 7 giugno 1965, 381 U.S. 4797 Giugno 1965) quando la privacy ha iniziato ad essere considerata come espressione del principio di autodeterminazione dell'individuo.

[43]Cfr. M. NOWAK, *op. cit.*, v. sopra nota 37, pag. 378.

Nel panorama europeo il problema della protezione dei dati ha iniziato a palesarsi nel periodo successivo alla fine del secondo conflitto mondiale. Duranti i regimi totalitari erano state infatti raccolte, grazie all'ascolto delle conversazioni telefoniche e alla raccolta sistematizzata dei dati, enormi quantità di informazioni riguardanti le vite private dei propri cittadini[44]. Il controllo di massa messo in atto dai suddetti regimi aveva generato nel popolo europeo una forte coscienza circa il bisogno di proteggere i dati personali, ritenuti fondamentali al fine di salvaguardare, a loro volta, le altre libertà fondamentali e la democrazia. A questo proposito è molto importante sottolineare che, a differenza del continente americano dove la privacy si è originata come *right to be left alone,* in Europa essa è legata al diritto dell'individuo a non essere sottoposto a controlli e raccolta di informazioni senza il suo consenso.

Successivamente, a partire soprattutto dagli anni '60, la dottrina ha iniziato ad interrogarsi sulle conseguenze che l'utilizzo massiccio dei computer per il trattamento dei dati personali avrebbe potuto comportare sulla vita privata delle persone[45]. Il problema dell'impatto della tecnologia sui diritti umani era già stato d'altronde evidenziato in quegli stessi anni anche dai principali organi internazionali[46]. Appare infatti appena il caso di ricordare che la Proclamazione di Teheran, adottata in seno alla Conferenza internazionale sui diritti umani del 1968, constatava al paragrafo 18 che "[...] while recent scientific discoveries and technological advances have opened vast prospect for economic, social and cultural progress, such developments may nevertheless endanger the rights and freedoms of individuals and will require continue attention"[47]. Pochi anni più tardi, nel 1975, l'Assemblea generale delle Nazioni Unite adottava la *Dichiarazione sull'utilizzo dei progressi della scienza e della tecnica nell'interesse della pace e a beneficio dell'umanità*[48]*,* sulla base degli studi condotti da esperti dell'Organizzazione e presentati alla Commissione per i diritti umani del 1974, in cui gli Stati membri venivano invitati ad

[44]I primi strumenti per archiviare e conservare i dati, rappresentati da schede perforate e sistemi di elaborazione, era stati realizzati dalla società americana IBM. Sul rapporto tra l'utilizzo delle macchine di archiviazione americana e la persecuzione degli ebrei cfr. E. BLACK, *L'IBM e l'olocausto*, traduzione a cura di R. Zuppet e S. Mancini, Rizzoli, Milano 2001.

[45]Cfr. F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali, Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino 2016, pag. 12.

[46]Cfr. F. MARTINES, *La Protezione degli Individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione Europea*, in *Rivista Italiana di Diritto Pubblico Comunitario* 2000, pag. 723 e ss.

[47]Proclamazione di Teheran, *Final Act of the International Conference on Human Rights*, Teheran, 22 aprile–13 maggio 1968, A/CONF. 32/41 at 3 (1968).

[48]Assemblea Generale delle Nazioni Unite, *Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind*, 10 novembre 1975, Risoluzione n. 3384 (XXX).

adottare misure appropriate al fine di evitare che il progresso scientifico e tecnologico potesse interferire, e conseguentemente limitare, il godimento dei diritti umani così come sanciti nella Dichiarazione universale dei diritti umani e nelle principali convenzioni internazionali. Invero, come ha anche avuto modo di sottolineare la sottocommisione nominata dalla Commissione per i diritti umani nel 1977[49], lo sviluppo dei sistemi informatici e dei computer aveva comportato un ricorso sempre più massiccio agli archivi elettronici e, conseguentemente, anche ai dati personali. Attraverso gli strumenti informatici, anche le pubbliche amministrazioni nazionali avevano iniziato ad accrescere le proprie capacità di raccogliere ed archiviare delle informazioni personali[50]. Oltre agli evidenti vantaggi in termini di velocità ed economicità, si materializzava in maniera sempre più evidente il rischio che la disponibilità degli stessi fosse soggetta ad abusi[51].

Si consideri inoltre che i mezzi e la frequenza con cui le persone possono comunicare sono cresciuti in modo esponenziale negli ultimi decenni. In particolare, si è assistito al passaggio dal telefono fisso al telefono mobile[52] e, parallelamente, all'avvento e allo sviluppo di Internet. Questi fattori, se da un lato hanno comportato una diminuzione dei costi delle comunicazioni – facilitando, conseguentemente, il flusso di informazioni e di idee a livello globale e aumentando anche le opportunità di crescita economica e sociale - dall'altro lato hanno accresciuto le possibilità per gli Stati di monitorare e sorvegliare i propri cittadini[53]. Internet ha infatti facilitato lo sviluppo di un grande numero di "transactional data", i quali possono essere immagazzinati, resi accessibili e ricercabili da

[49]Cfr. E. LAWSON, *Encyclopedia of Human Rights,* Taylor Francis, Washington DC 1996, pag. 1195.
[50]Cfr. A. R. MILLER, *The assault on privacy: computers, data banks, and dossiers,* The University of Michigan Press, Michigan 1971, pag. 13 e ss. In realtà, già in passato i soggetti privati come banche e professionisti, e le pubbliche amministrazioni a partire dall'epoca napoleonica, raccoglievano una grande quantità di informazioni personali. Queste, venivano, però, raccolte e gestite solitamente da un'unica autorità pubblica locale ed era materialmente più difficile diffonderle altrove. Si aggiunga, inoltre, che il soggetto poteva facilmente sottrarsi alla raccolta, o essere facilmente "dimenticato", semplicemente nascondendosi o trasferendosi in un'altra città. Ad oggi, invece questo risulta pressoché impossibile nelle società informatizzate. Cfr. anche F. PIZZETTI, *op. cit.*, v. sopra nota 45, pag. 13.
[51]Nel contesto americano, il fenomeno della raccolta delle informazioni personali ha iniziato a manifestarsi con l'inserimento del governo nelle sfere della tassazione e del sociale. Poi, con l'avvento della tecnologia e la possibilità di immagazzinare una grande quantità di dati personali in maniera sempre più rapida ed economica, l'operato del governo si è fatto più massico e ne sono prova l'incremento dei questionari cui erano soggetti gli individui e le società di ogni grandezza e forma. Secondo Miller, già nei lontani anni '60 "*the electronic technology is trasnforming the world into a "global village" in which the demain of strictly private action is steadily being eroded"* (A. R. MILLER, *op. cit.*, v. sopra nota 50, pag. 21).
[52]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, 23esima sessione, 17 Aprile 2013, A/HRC/23/40, par. 13.
[53]Consiglio per i diritti umani, *ibidem*, par. 11.

chiunque. Nel corso degli ultimi decenni, il concetto di privacy è andato dunque espandendosi ricomprendendo anche quella nuova dimensione della vita privata dell'individuo rappresentata dai suoi dati personali, conservati ed utilizzati per fini diversi da soggetti terzi[54]. All'originario *right to be let alone* si è infatti aggiunto il diritto di controllare l'uso che gli altri fanno dei propri dati personali[55]. Per l'esattezza, il passaggio è stato: diritto alla riservatezza, diritto all'identità personale, diritto all'autodeterminazione informatica e, infine, diritto al trattamento dei propri dati personali. Quest'ultimo ricomprende a sua volta tre sottocategorie di diritti: il diritto alle informazioni, ossia il diritto ad avere accesso ai propri dati; il diritto ad essere informati sulle finalità e modalità dei trattamenti relativi ai propri dati; il diritto ad acconsentire o negare alla raccolta e all'uso delle informazioni che lo riguardano, salvo i casi in cui queste attività siano consentite per ragioni particolari definite dalla legge. Si può ritenere, pertanto, che mentre il diritto alla privacy si è originato dal bisogno degli individui di proteggere dalle intrusioni esterne, quello alla protezione dei dati personali è derivato dalla necessità di controllare l'uso che gli altri fanno delle proprie informazioni[56].

Orbene, nell'attuale connotazione, il termine "protezione dei dati personali" sta ad indicare, in generale, l'insieme delle norme finalizzate a gestire e a proteggere il flusso di informazioni relative alle persone fisiche - restando escluse quelle concernenti le persone giuridiche[57]. Il graduale processo di "smaterializzazione" della privacy da una concezione fortemente legata al diritto di proprietà verso una nuova caratterizzata dalla protezione dei dati personali ha di fatto comportato una scorporazione dei due diritti in questione. Se da un lato, infatti, esiste un diritto legato all'individualità e al bisogno di protezione del proprio ambiente domestico da qualsiasi interferenza esterna, dall'altro lato i dati personali diventano elementi autonomi di tutela, dotati di un proprio valore e scambiabilità[58].

[54]Grazie allo sviluppo sempre più avanzato delle tecnologie, i costi da affrontare per la raccolta di dati sono diventati più competitivi.
[55]Cfr. R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè 2003, pag. 6; F. PIZZETTI, *op. cit.*, v. sopra nota 45, pag. 13.
[56]Cfr. H. HIJMANS, *The European Union as Guardian of Internet Privacy*, Springer International Switzerland 2016, pag. 48 e ss.
[57]Cfr. D. DOERR, RUSSEL L, WEAVER, *Perspective on Privacy, increasing Regulation in the Usa, Canada, Australia and European Countries*, De Gruyter, Berlin/Boston 2014, pag. 47
[58]Differenza resa evidente dalla previsione, nella Carta dei diritti fondamentali dell'Unione europea, di due diversi articoli, uno per il diritto alla privacy e l'altro per il diritto alla protezione dei dati personali. Cfr. M. TZANOU, *Data Protection as a fundamental right next to privacy? Reconstructing' a not so new right*, in *International Data Privacy Law*, 2016, pag. 89 e J. KOKOTT E C. SOBOTTA, *The distinction between*

Occorre rilevare però che - come si avrà d'altronde modo di analizzare in maniera approfondita nel prosieguo del presente elaborato grazie all'analisi comparata delle diverse fonti legislative internazionali ed regionali che tutelano la privacy - non tutti gli ordinamenti giuridici hanno riconosciuto il venire meno dell'unitarietà di tale diritto e continuano, pertanto, a tutelare la vita privata e familiare e i dati personali nella stessa disposizione normativa.

Malgrado l'evidente importanza rivestita dal diritto in questione, e i numerosi profili di criticità emersi in seguito ai recenti avvenimenti in materia di sorveglianza di massa – destinati ad aumentare in ragione di una società sempre più digitalizzata ed informatizzata - risulta tuttora difficile delinearne in modo esaustivo il contenuto[59] e non esiste al riguardo una definizione universale, né tanto meno una convenzione di tale portata - prevista, invece, per altri diritti umani quali il divieto di tortura e trattamenti inumani e degradanti, il divieto di discriminazione, i diritti del fanciullo, il diritto ad un ambiente sano. Com'è stato infatti finora evidenziato, la vaghezza del concetto di privacy deriva principalmente dal fatto che essa si sviluppa ed amplia di pari passo con il progresso scientifico-tecnologico raggiunto da una determinata collettività organizzata, in particolare dal grado di sviluppo ed impiego delle cosiddette tecnologie dell'informazione e della comunicazione[60]. L'utilizzo di questi strumenti è infatti capace di modificare la percezione che gli individui hanno della propria sfera privata, favorendo il rimodellando del diritto stesso. Lo sviluppo tecnologico è anche coinciso con un significativo cambiamento sociale nella nozione di privacy. L'avvento dei *social media* ha dato ad ognuno uno spazio in cui rivelare le proprie informazioni personali ad una vasta e permanente scala di persone. L'invadenza dei *social media* ha di fatto cambiato la percezione individuale e sociale di ciò che deve essere la vita privata[61]. Sotto questo profilo appare molto interessante l'opinione espressa da Focarelli,

---

privacy and data protection in the jurisprudence of the CJEU and the ECtHR, in *International Data Privacy Law* 2017, pagg. 222-228.

[59]Cfr. A. R. MILLER, *op. cit.*, v. nota sopra 50, pagg. 25 e ss.

[60]Cfr. A. DI MARTINO, *La protezione dei dati personali*, in S.P. PANUNZIO, *I diritti fondamentali e le Corti in Europa,* Jovene, Napoli 2005, pag. 730. Sulla natura controversa del diritto cfr. anche N. WITZLEB, D. LINDSAY, M. PATERSON, S. RODRICK, *op. cit.,* v. sopra nota 2, pag. 1 e ss.

[61]Cfr. C. FOCARELLI, *La persona umana nel diritto internazionale*, il Mulino, Bologna 2013, pag. 171. Questo aspetto è stato confermato anche dall'Alto Commissario delle Nazioni Unite per i diritti umani, Navi Pillay, durante la sessione del 24 febbraio 2014. Essa ha infatti sottolineato che "As civic life increasingly is conducted online in this digital age, some have questioned the relevance of the notion of privacy. Some have suggested that the conveyance and exchange of personal information via electronic means is part of a conscious compromise. Individuals voluntarily surrender information about themselves and their

secondo cui si è assistito negli ultimi anni ad una vera cessione volontaria da parte degli individui della propria privacy, vuoi per motivi economici vuoi per motivi di fama, per cui non si può più parlare di "violazione" quanto piuttosto di "vendita", deliberata o meno, della propria vita privata[62]. Sempre secondo l'autore "[…] Il problema oggi non è lo strapotere dello stato ma lo strapotere del singolo, o meglio l'influenza persuasiva – anche nell'uso di internet e dei messaggi spontaneamente immessi in rete – dei centri di potere politico ed economico, con la loro propaganda a favore di un'apparente illimitata libertà individuale, grazie alla loro capacità di pilotare le scelte individuali […]"[63].

Il diritto alla privacy nell'era digitale può essere ricondotto principalmente a due tipi di sottocategorie, rappresentate dalla "privacy dell'informazione" e dalla "privacy delle comunicazioni" - definiti dalla dottrina americana rispettivamente "Information Privacy" e "Decisional Privacy"[64]. La privacy dell'informazione è quella relativa alla raccolta, all'accesso e alla conservazione dei dati personali - quale può essere la documentazione medica e finanziaria - mentre la privacy delle comunicazioni concerne le e-mail, i messaggi di testo, le comunicazioni su Internet (per esempio i blog), telefoni cellulare e ogni altra forma di comunicazione che utilizza i mezzi di diffusione[65]. Entrambi i tipi di privacy necessitano protezione e riconoscimento.

E' inoltre ormai pacifico che il diritto alla privacy e alla protezione dei dati personali siano due diritti autonomi da trattare in maniera distinta. Questa differenziazione, riprodotta a livello normativo solo nella Carta dei diritti fondamentali dell'Unione europea, che tutela i due diritti in questione rispettivamente all'articolo 7 e all'articolo 8, costituisce, invece, nel sistema di tutela internazionale dei diritti umani previsto dal Patto sui diritti civili e politici e quello regionale previsto dalla CEDU, il frutto di elaborazioni giurisprudenziali e dottrinali. Secondo parte della dottrina, in particolare, il diritto alla protezione dei dati personale sarebbe più ampio e, allo stesso tempo, più specifico rispetto a quello alla privacy. Più ampio in quanto ricomprenderebbe anche la tutela di altri diritti umani quali la libertà di espressione e la libertà religiosa; più specifico, invece, in quanto

---

relationships in return for digital access to goods, services and information". Per il testo integrale cfr. http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14276&LangID=E#main).

[62]Cfr. C. FOCARELLI, *op. cit.*, v. sopra nota 61, pag. 171.

[63]*Ibidem,* pag. 172.

[64]M. SCHACHTER, *Informational and Decisional Privacy*, Carolina Academic Press 2003, pag. 288.

[65]Cfr. R. C. OWENS, *Human Rights and the Internet, Balance and exercise of fundamental rights online*, in *Computer and Law Review* 2008, pag. 161.

avrebbe un oggetto più definito rappresentato dai dati personali nel momento in cui questi vengono trattati[66].

1.5 LA TUTELA DEI DATI PERSONALI NEL DIRITTO INTERNAZIONALE

Prima di procedere all'analisi delle fonti del diritto internazionale che tutelano la privacy, si rende opportuno fare due premesse, una di carattere contenutistico e una di carattere metodologico.

Per quanto riguarda il primo aspetto, occorre tenere presente che nel diritto internazionale la nozione di "privacy" è molto ampia e non ancora definita in maniera esaustiva. Essa si articola infatti in diverse sottocategorie che riguardano aspetti o elementi diversi della vita dell'individuo: la sua identità ed integrità fisica, la vita familiare, il comportamento ed orientamento sessuale, la corrispondenza, l'onore e la reputazione e, infine, i dati personali[67]. Quest'ultima sottocategoria sta acquisendo una sempre maggiore autonomia e al riguardo è indicativa la distinzione già operata in alcune fonti regionali quali la Carta dei diritti fondamentali dell'Unione europea, ove la vita privata e familiare è disciplinata all'articolo 7 mentre i dati personali all'articolo 8.

Dal punto di vista metodologico, si procederà all'analisi della disciplina giuridica partendo dalle norme a carattere "universale" – ossia dalle fonti internazionali sia di natura pattizia che di *soft law* - per poi passare a quelle regionali, rappresentate principalmente dalla CEDU e dal diritto dell'Unione europea. Inoltre, ove prevista, tutte le fonti del diritto verranno analizzate mettendo in rilievo la c.d. *clausola di deroga o limitazione*, che si concretizza nella possibilità riconosciuta in capo agli Stati di limitare di volta in volta il diritto alla privacy per le diverese ragioni ritenute legittime e necessarie. Infatti, come si avrà modo di evidenziare in seguito, la privacy è un diritto relativo[68] e tutte le fonti legislative in materia ammettono, in maniera più o meno esplicita, la possibilità di invocare la suddetta deroga.

---

[66]Cfr. S. GUTWIRTH, Y. POULLET, P. DE HERT, *Data Protection in a Profiled World,* Springer Netherlands 2010, pag. 37.

[67]M. NOWAK, *op. cit.*, v. sopra nota 37, pag. 377-405.

[68]La relatività del diritto alla privacy è già stata evidenziata dagli organi internazionali di controllo nel 1988, quando il Comitato per i diritti umani ha pubblicato il *General Comment no. 16*: *Article 17* (*Right to Privacy)*, 8 aprile 1988, HRI/GEN/1/Rev. 9.

Occorre fin da subito precisare che l'autore, nonostante accolga l'ormai consolidata concezione europea secondo cui vi è una netta distinzione fra diritto alla privacy e diritto alla protezione dei dati personali – impostazione resa evidente anche nella Carta dei diritti fondamentali dell'Unione europea, che disciplina i relativi diritti in due distinti articoli[69] - userà spesso, per semplicità della trattazione, i termini come sinonimi, anche alla luce del fatto che sia nella CEDU sia nel Patto sui diritti civili e politici i due diritti restano tutelati dalla stessa norma. Con l'ulteriore precisazione, però, che in questo contesto la privacy viene sempre e solo intesa come protezione dei dati personali e non nelle altre sottocategorie.

A livello internazionale, la privacy viene tutelata innanzitutto dall'articolo 12 della Dichiarazione universale dei diritti umani e dall'articolo 17 del Patto sui diritti civili e politici. Orbene, prima di procedere analisi delle due fonti giuridiche appena menzionate, occorre fare un'ulteriore premessa di natura metodologica: si è ritenuto opportuno analizzare l'articolo 12 della Dichiarazione universale dei diritti umani, la più importante fonte di *soft law* in materia di tutela dei diritti umani, in comparazione con l'articolo 17 del Patto sui diritti civili e politici, fonte invece di *hard law*, in ragione delle numerose analogie testuali che le stesse presentano, che ne facilitano quindi una trattazione congiunta.

Le due norme hanno, infatti, un contenuto pressoché identico e sanciscono entrambe il diritto per ogni individuo a non essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesioni del suo onore e alla sua reputazione. Ogni individuo, inoltre, ha il diritto ad essere tutelato dalla legge contro le suddette interferenze o lesioni[70].
Nonostante la Dichiarazione universale sia priva di efficacia giuridica vincolante, in quanto adottata tramite una risoluzione dell'Assemblea generale delle Nazioni Unite[71], essa rappresenta il documento internazionale contenente un elenco di diritti umani avente

[69]Articolo 8 Carta dei diritti fondamentali dell'Unione europea" Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".
[70]Articolo 12 Dichiarazione universale dei diritti umani e articolo 17 Patto sui diritti civili e politici.
[71]Assemblea delle Nazioni Unite, 10 dicembre 1948, Risoluzione A/RES/3/217 A.

portata universale[72] e ha costituito la premessa per l'adozione dei successivi trattati internazionali sui diritti umani - in particolare, per il Patto sui diritti civili e politici e il Patto sui diritti economici sociali e culturali - dotati questi ultimi, al contrario, di efficacia giuridica vincolante, nonché per i trattati regionali come la CEDU. Infatti, al fine di garantire il rispetto dei diritti umani in essi sanciti, sono stati previsti organi internazionali di controllo, quali, rispettivamente, il Comitato per i diritti umani e il Comitato sui diritti economici, sociali e culturali (CESCR). Allo stesso modo, la CEDU prevede quale organo di controllo la Corte europea dei diritti umani, la quale ha assunto una notevole rilevanza negli ultimi decenni – data la crescita esponenziale dei ricorsi presentati alla stessa dai singoli individui per asserita violazione dei loro diritti fondamentali – e, come si avrà modo di approfondire nel proseguo della presenta trattazione, ha determinato gli standard minimi in materia di tutela dei dati personali in tutto il contesto giuridico europeo.

Tornando all'analisi dell'articolo 17 del Patto sui diritti civili e politici, esso si differenzia dalla Dichiarazione, in quanto presenta un secondo comma ove viene disposto che "Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese". L'articolo in esame è stato oggetto del *General Comment no. 16* da parte del Comitato per i diritti umani nel 1988[73], in cui è stato specificato, tra le altre cose, che il diritto alla privacy debba essere protetto da ogni interferenza o attacco, sia esso promanante da un'autorità statale o da una persona naturale o giuridica. Inoltre, sempre in base al *General Comment*, può ritenersi che dall'articolo 17 discenda in capo agli Stati membri contraenti un duplice obbligo, uno di natura negativa e uno di natura positiva: se da un lato, infatti, le autorità pubbliche devono evitare qualsiasi interferenza arbitraria o

[72]Cfr. L. PINESCHI, *La tutela internazionale dei diritti umani, norme, garanzie, prassi,* Giuffré, Milano 2015, pag. 67 e ss. Sul punto in realtà la dottrina non è del tutto unanime. Secondo alcuni, infatti, la Dichiarazione, pur priva di efficacia giuridica vincolante, può considerarsi una specificazione degli obblighi generali di tutela dei diritti umani che gli Stati hanno assunto nel stipulare la Carta delle Nazioni Uniti. Conseguentemente, una violazione dei principi in essa sancita costituirebbe violazione degli obblighi generali di cooperazione di cui dall'articolo 56 della Carta. L'importanza fondamentale assunta dalla Dichiarazione universale dei diritti umani nel contesto giuridico internazionale è, inoltre, dimostrata dal fatto che i diritti in essa sanciti sono stati trasposti nella maggior parte delle Costituzioni e statuti dei paesi firmatari e utilizzati da numerosi Tribunali nazionali quale parametro interpretativo della legge statale. Secondo alcuni, il continuo richiamo ai diritti della Dichiarazione costituisce una prova evidente del loro valore di diritto consuetudinario internazionale, che è legalmente vincolante a tutti gli effetti. Un ragionamento di questo tipo può essere svolto sicuramente con riguardo al divieto di tortura, il quale ha assunto a tutti gli effetti valore di *ius cogens.* Si vedano, *inter alia*, M. GLEN JOHNSON, J. SYMONIDES, *The Universal Declaration of Human Rights*, *A history of its creation and implementation 1948*-1998, UNESCO Publishing 1998; B.G. RAMCHARAN, *Human Rights- Thirty years after the Universal Declaration*, Martinus Nijhoff Publishers 1979.

[73]Comitato per i diritti umani, *General Comment no. 16*: *Article 17 (Right to Privacy)*, 8 Aprile 1988, HRI/GEN/1/Rev. 9.

illegittima nella vita privata, dall'altro lato ad esse è demandato il compito di adottare misure legislative idonee a tutelare gli individui da queste interferenze, nel rispetto dei limiti e degli obiettivi della Convenzione[74].

Dal punto di vista contenutistico, il Patto sui diritti civili e politici introduce, rispetto alla Dichiarazione universale dei diritti umani, un'importante novità rappresentata dall'aggettivo "illegittimo", che qualifica sia l'interferenza nella vita privata, nella famiglia, nella casa e nella corrispondenza, sia l'offesa all'onore e alla reputazione. Invero, secondo quanto specificato dal Comitato, con il termine "illegittimo" si fa riferimento al fatto che nessuna misura di sorveglianza possa essere adottata se non nei casi in cui è espressamente prevista dalla legge[75]. La suddetta legge è soggetta, quindi, ad un duplice giudizio di conformità, ovvero sia agli obiettivi e alle finalità del Patto che alla legge nazionale. Il termine "interferenza arbitraria" ha invece un'eccezione più ampia, ricomprendendo anche i casi in cui la misura, pur essendo stata adottata attraverso uno strumento legislativo, non è in linea con gli obiettivi e le finalità del Patto.

All'interno dell'articolo viene poi operata un'ulteriore differenziazione tra l'interferenza nella vita privata, famiglia e corrispondenza da una parte, e nell'onore e reputazione dall'altra, attribuendo alla prima una maggiore importanza rispetto alla seconda. In particolare, nel primo comma viene vietata qualsiasi interferenza qualificabile come "arbitraria" ed "illegittima", mentre nel secondo comma sono vietate interferenze all'onore e alla reputazione unicamente se "illegittime"[76]. Si ritiene che esista, pertanto, una vera e propria gerarchia tra i due diversi interessi tutelati, che si giustifica in ragione del fatto che il rispetto dell'onore e della reputazione, a differenza del diritto alla vita privata e familiare, debba essere bilanciato con un altro diritto fondamentale sempre tutelato dal Patto, ossia la libertà di espressione[77].

---

[74]Un obbligo analogo discende anche dall'articolo 8 CEDU.

[75]Comitato per i diritti umani, *General Comment no. 16*: *Article 17 (Right to Privacy)*, 8 Aprile 1988, HRI/GEN/1/Rev. 9, parr. 8 e 9.

[76]Cfr. M. NOWAK, *op. cit.*, v. sopra nota 37, pag. 381.

[77]Articolo 19 Patto sui diritti civili e politici "1. Ogni individuo ha diritto a non essere molestato per le proprie opinioni. 2. Ogni individuo ha il diritto alla libertà di espressione; tale diritto comprende la libertà di cercare, ricevere e diffondere informazioni e idee di ogni genere, senza riguardo a frontiere, oralmente, per iscritto, attraverso la stampa, in forma artistica o attraverso qualsiasi altro mezzo di sua scelta. 3. L'esercizio delle libertà previste al paragrafo 2 del presente articolo comporta doveri e responsabilità speciali. Esso può essere pertanto sottoposto a talune restrizioni che però devono essere espressamente stabilite dalla legge ed essere necessarie: a) al rispetto dei diritti o della reputazione altrui; b) alla salvaguardia della sicurezza nazionale, dell'ordine pubblico, della sanità o della morale pubbliche".

Occorre infine sottolineare che il *General Comment*, pur provvedendo a definire i concetti di arbitraria e illegittima interferenza, omette di indicare le modalità effettive con cui gli Stati possono proteggere gli individui dalle suddette misure, delegando quindi alle autorità statali il compito di definirne le specifiche modalità tramite gli organi legislativi, amministrativi e giudiziari[78].
In ogni caso, tranne l'introduzione dell'aggettivo "illegittimo" e la suddivisione dell'articolo in due distinti paragrafi, le disposizioni della Dichiarazione universale dei diritti umani e del Patto sui diritti civili e politici risultano identiche.

Si rileva, infine, che sia la Dichiarazione universale che il Patto sui diritti civili e politici non prevedano espressamente, a differenza dell'articolo 8 CEDU, alcuna clausola di restrizione, limitandosi ad una mera enunciazione del diritto in questione e alla necessità di proteggerlo da qualsiasi interferenza illegittima.
Per quanto riguarda l'articolo 17 del Patto sui diritti civili e politici, le clausole di limitazione si ricavano, tuttavia, in maniera implicita dagli aggettivi "arbitraria" ed "illegittima". Questi aggettivi renderebbero di fatto possibile, *a contrarii*, ogni misura di limitazione, a condizione che essa non sia arbitraria e sia stata legittimamente adottata. In ragione di ciò, la privacy deve considerarsi un diritto relativo, contrapposto ad altri invece assoluti, rappresentati nella fonte appena analizzata, ad esempio, dal divieto di schiavitù e dal principio dell'irretroattività della legge penale. L'articolo 17 deve essere, inoltre, letto in combinato disposto con un altro *General Comment* redatto dal Comitato per i diritti umani, relativo alla *natura delle obbligazioni imposte dalla Convenzione in capo agli Stati membri*[79], il quale stabilisce al paragrafo 6 che "[…] any restrictions on any of those rights must be permissible under the relevant provisions of the Covenant. Where such restrictions are made, States must demonstrate their necessity and only take such measures as are proportionate to the pursuance of legitimate aims in order to ensure continuous and effective protection of Covenant rights. In no case may the restrictions be applied or invoked in a manner that would impair the essence of a Covenant right". Dalla suddetta disposizione discendono i tre principi fondamentali in materia di deroghe: a)

[78]Cfr. E. LAWSON, *Encyclopedia of Human Rights,* Taylor Francis, Washington DC 1996, pag. 1194.
[79]Comitato per i diritti umani, *General Comment no. 31*, *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 26 maggio 2004, CCPR/C/21/Rev.1/Add. 1326.

proporzionalità; b) necessità; c) rispetto dell'essenza dei diritti previsti dalla Convenzione[80].

Infine, viene in rilievo il recente rapporto dello *Special Rapporteur* sul diritto alla libertà di espressione[81] adottato dal Consiglio per i diritti umani delle Nazioni Unite nel 2013, il quale ha ulteriormente specificato i limiti da rispettare in caso di limitazioni al diritto alla privacy. In particolare, è stato stabilito che ogni restrizione debba essere prevista dalla legge e non danneggiare l'essenza del diritto umano in questione. Inoltre le restrizioni devono essere necessarie e perseguire uno scopo legittimo, nonché proporzionate rispetto ai fini perseguiti[82].

Anticipando inoltre quello che costituirà oggetto di trattazione del proseguo della presente trattazione, occorre sottolineare che il diritto alla privacy, oltre ad essere relativo, è anche derogabile. Esso può infatti costituire, in particolari situazioni di emergenza, oggetto di deroga ai sensi dell'articolo 4 del Patto sui diritti civili e politici e dell'articolo 15 CEDU.

1.5.1 La Convenzione sui diritti del fanciullo e la Convenzione internazionale sulla protezione dei diritti dei lavoratori migranti

Sempre a livello internazionale, il diritto alla privacy viene sancito anche nella Convenzione sui diritti del fanciullo, adottata dall'Assemblea generale delle Nazioni Unite il 20 novembre 1989[83]. In particolare, all'articolo 16 stabilisce che: "1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation. 2.The child has the right to the protection of the law against such interference or attacks".

[80]Un altro strumento senz'altro utile al fine di delimitare la portata della deroga in esame è rappresentato dai *Siracusa Principles on the Limitation and Derogation Provisions in the International Covenant on Civil and Political Rights*, adottati dall'American Association for International Commission of Jurist nel 1985, disponibile alla pagina http://icj.wpengine.netdna-cdn.com/wp-content/uploads/1984/07/Siracusa-principles-ICCPR-legal-submission-1985-eng.pdf.

[81]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, 23esima sessione, 17 Aprile 2013, A/HRC/23/40.

[82]I*bidem*, par. 29. Lo *Special Rapporteur* ritiene che questi principi, previsti in realtà con riferimento alla libertà di movimento, siano pacificamente applicabili anche al diritto alla privacy.

[83]Adottata tramite risoluzione n. 44/25 e ratificata in Italia con la legge 27 maggio 1991, n. 176. La Convenzione sui diritti dell'infanzia e dell'adolescenza è considerato il primo strumento internazionale giuridicamente vincolante in materia di protezione dei diritti dei minori. Testo integrale disponibile alla pagina http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx.

A differenza della Dichiarazione universale dei diritti umani e del Patto sui diritti civili e politici, la presente Convenzione identifica il soggetto titolare del diritto, che è, nel caso di specie, il fanciullo. Per quanto riguarda invece il significato da attribuire alle nozioni di interferenza "arbitrary" e "unlawful", valgono le stesse considerazioni svolte nel paragrafo precedente in merito all'articolo 17 del Patto sui diritti civili e politici – cui si rinvia integralmente[84].

Si ricorda, infine, la Convenzione internazionale sulla protezione dei diritti dei lavoratori migranti e dei membri delle loro famiglie, adottata dall'Assemblea generale delle Nazioni Unite il 18 dicembre 1990[85] ed entrata in vigore il primo luglio 1990, che sancisce il diritto alla tutela della vita privata e familiare all'articolo 14. La suddetta disposizione normativa prevede, in particolare, che: "No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks".

1.5.2 Le fonti di *soft law*

Nel sistema internazionale di tutela dei diritti umani, il diritto alla tutela dei dati personali viene disciplinato non solo da trattati e convenzioni, ma anche dalle cosiddette fonti di *soft law,* che si caratterizzano per il loro carattere non vincolante.

Orbene, a livello cronologico, la prima fonte *di soft* law che riconosce a livello internazionale il diritto alla privacy è la Dichiarazione universale dei diritti umani, approvata e proclamata nel 1948 e già oggetto di analisi nel paragrafo precedente.
Successivamente, il 14 dicembre 1990, l'Assemblea generale delle Nazioni Unite ha pubblicato le *Guidelines for the Regulation of Computerized Personal Data Files*[86]. Così come la Dichiarazione universale dei diritti umani, questo documento è stato adottato con

[84]Cfr. S. DETRICK, *A commentary on the United Nations Convention on the Rights of the Child*, Martinus Nijhoff Publishers, Leida 1999, pag. 269-282. Cfr. Anche S. DETRICK, *The United Convention on the Rights of the Child, a Guide to the "Travaux Préparatoires*", Martinus Nijhoff Publishers, Leida 1992, pag. 255-262.
[85]Convenzione internazionale sulla protezione dei diritti dei lavoratori migranti e dei membri delle loro famiglie, adottata Assemblea Generale delle Nazioni Unite con risoluzione 45/158 del 18 dicembre 1990. Testo integrale disponibile alla pagina http://www.ohchr.org/EN/ProfessionalInterest/Pages/CMW.aspx.
[86]Assemblea Generale delle Nazioni Unite, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 dicembre 1990, Risoluzione 45/95.

una risoluzione dell'Assemblea generale ed è, pertanto, privo di efficacia giuridica vincolante.
Il documento si compone principalmente di due parti: nella prima vengono enunciati i principi regolatori relativi al trattamento di informazioni personali degli individui contenuti in archivi informatici, i quali dovrebbero essere a loro volta recepiti dalle legislazioni degli Stati membri delle Nazioni Unite; nella seconda parte, invece, viene definito il suo ambito di applicazione.

Per quanto riguarda la prima parte, i più importanti principi ivi sanciti sono, in particolare, la legittimità e la correttezza nella raccolta ed elaborazione dei dati (articolo 1), il diritto di accesso da parte dell'interessato (articolo 4), il principio di non discriminazione (articolo 5), la previsione all'interno di ciascun stato membro di un'"autorità indipendente e imparziale" (articolo 8), il principio generale di libera circolazione transfrontaliera dei dati, (articolo 9). Inoltre, all'articolo 6 è prevista la cosiddetta *clausola umanitaria*, ossia la possibilità in capo agli Stati di limitare il diritto alla privacy per ragioni connesse alla sicurezza nazionale, all'ordine pubblico, alla salute e morale pubblica e per i diritti e le libertà degli altri individui, specialmente quelli perseguitati. In base, invece, a quanto previsto dall'articolo 8, ogni stato membro deve dotarsi nel proprio ordinamento di un'"autorità indipendente e imparziale", con il compito di supervisionare il rispetto dei summenzionati principi e di sanzionare le eventuali violazioni (articolo 8). Il principio generale della circolazione transfrontaliera dei dati, in base al quale i dati possono circolare liberalmente tra diversi Paesi solo nella misura in cui questi garantisca un equiparato livello di tutela (articolo 9).
Dall'appena menzionato elenco emerge che anche le *Guidelines* prevedono all'articolo 6, al pari delle fonti internazionali di *hard law* finora analizzate, la possibilità di limitare la protezione dei dati personali e questo costituisce ulteriore prova della natura relativa del diritto in questione.
La seconda parte del documento riguarda invece l'applicazione del contenuto delle *Guidelines* anche alle organizzazioni intergovernative, che deve tenere conto, tra le altre cose, delle differenze intercorrenti tra gli archivi utilizzati per fini interni – come potrebbero essere quelli relativi al personale – e quelli utilizzati per fini esterni, relativi soprattutto ai soggetti terzi che intrattengono rapporti con le organizzazioni. Ogni organizzazione deve inoltre nominare un'autorità indipendente che ha il compito di

supervisionare l'osservanza delle *Guidelines*. È prevista infine anche nei confronti delle organizzazioni la cosiddetta clausola umanitaria.

Il primo documento ufficiale in materia di tutela della privacy adottato dal Comitato per i diritti umani risale al 1988, quando è stato pubblicato il *General Comment no. 16*: *Article 17 (Right to Privacy)*[87], che ha costituito, tra l'altro, oggetto di analisi nei paragrafi precedenti del presente elaborato[88] - cui si fa integralmente rinvio.

Negli ultimi anni, in ragione dell'inarrestabile sviluppo tecnologico e delle rivelazioni del fenomeno della sorveglianza di massa da parte dell'*ex* agente dell'NSA Snowden, il dibattito circa la necessità di tutelare la privacy contro le interferenze illegittime da parte delle autorità statali ha riacquisito un significativo interesse anche all'interno delle Nazioni Unite.

In particolare, il 17 aprile 2013 è stato pubblicato il rapporto dello Special Rapporteur delle Nazioni Unite sulla *promozione e protezione della libertà di opinione ed espressione di Frank La Rue*[89], nel quale sono state analizzate le implicazioni della sorveglianza delle comunicazioni sulla libertà di espressione e sulla privacy. È stato innanzitutto constatato come il recente sviluppo dei mezzi tecnologici abbia di fatto accresciuto le possibilità per gli Stati di controllare il flusso di informazioni scambiate fra i gli individui, facilitato anche dalla maggiore accessibilità e dall'abbassamento dei costi degli strumenti utilizzati per monitorare. A ciò si aggiunga il fatto che sia il sistema legislativo internazionale che quello nazionale non siano sempre in grado di tenere il passo allo sviluppo tecnologico e, conseguentemente, di legiferare in maniera adeguata e completa. La presenza di numerose lacune normative lascia quindi ampio margine di manovra agli Stati, che possono adottare misure sproporzionate e lesive dei diritti individuali[90].

Nel rapporto vengono messi in evidenza i due principali problemi connessi allo sviluppo tecnologico e alla possibilità di adottare misure di sorveglianza: la mancanza di un efficace ed effettivo controllo giurisdizionale[91] e il libero, e spesso arbitrario, ricorso alle clausole di deroga per la tutela della sicurezza nazionale. Lo *Special Rapporteur* sottolinea inoltre

[87]Comitato per i diritti umani, *General Comment no. 16: Article 17 (Right to Privacy)*, 8 aprile 1988, HRI/GEN/1/Rev. 9.
[88]Cfr. paragrafo 1.5.
[89]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, 23esima sessione, 17 aprile 2013, A/HRC/23/40.
[90]*Ibidem*, parr. 50-51.
[91]Inoltre, anche nei casi in cui la legge impone un'autorizzazione giudiziaria, questa è spesso *de facto* arbitraria (par. 56).

come le misure di interferenza debbano avere luogo solo "[…] under the most exceptional circumstances and exclusively under the supervision of an independent judicial authority"[92] ed essere, in ogni caso, rispettose dei principi di chiarezza, precisione, necessità, proporzionalità e base legislativa[93]. Gli Stati devono, in ogni caso, adottare delle misure legislative che facilitino il più possibile l'anonimizzazione delle comunicazioni. Sempre secondo lo *Special Rapporteur*, agli individui deve essere garantito il diritto a ricevere una notifica della misura di sorveglianza una volta che questa è terminata, al fine di garantire una tutela giurisdizionale in caso di sospette violazioni.
Infine, nel rapporto viene esortato il Comitato per i diritti umani ad adottare un nuovo *General Comment* relativo al diritto alla privacy, che vada a sostituire il *General Comment* n. 16 e tenga in considerazione, soprattutto, il ruolo sempre più preponderante assunto dagli attori privati[94].

Nel maggio 2015, il Consiglio per i diritti umani ha pubblicato il rapporto dell'Alto Commissario delle Nazioni Unite per i diritti umani, *The right to privacy in the digital* age[95], ove è stata dimostrata l'importanza della sicurezza digitale e della privacy al fine di garantire la libertà di espressione e di opinione nel mondo. Il rapporto ha inoltre evidenziato come la crittografia - il processo di scambio di informazioni codificate che solo autorizzate le persone possono visualizzare - e l'uso dell'anonimato possano rappresentare gli strumenti più efficaci per tutelare i suddetti diritti[96]. Al riguardo, preme richiamare l'acceso dibattito sorto negli ultimi mesi in merito alla possibilità per le società di telefonia di permettere l'accesso ai c.d. "backdoors" alle autorità statali. Si ricordi, infatti, il noto episodio dell'FBI contro Apple, in cui l'Ufficio Investigativo americano aveva chiesto di accedere alla c.d. "backdoor" di un *Iphone,* che era appartenuto presumibilmente ad uno dei fautori dell'attacco terroristico di San Bernardino del 2 dicembre 2015. La Apple negava l'accesso all'FBI, invocando come motivazione la necessità di non indebolire i sistemi crittografici al fine di tutelare in maniera più efficace la privacy di tutti gli utenti Apple.

[92] *Ibidem*, par. 81.
[93] *Ibidem,* par. 83.
[94] *Ibidem*, par. 98.
[95] Consiglio per i diritti umani, *Report of the Office of the United Nations High Commissioner for Human Rights*, *The right to privacy in the digital age*, 27esima sessione, 30 giugno 2014, A/HRC/27/37.
[96] Cfr. M. OROFINO, *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime,* in *DPCE online*, 2016-2, pag. 281.

Al pari dello *Special Rapporteur*, anche l'Alto Commissario evidenzia i rischi connessi alla comunicazione digitale – e alla corrispondente discesa dei costi per la memorizzazione e la raccolta dei dati da parte dei server – che ha di fatto reso possibile il controllo di massa da parte degli Stati su una scala senza precedenti[97]. Spesso, infatti, i governi giustificano il ricorso alle misure di sorveglianza delle comunicazioni per ragioni di sicurezza nazionale, tra cui vi rientra anche la minaccia terroristica. La sorveglianza può effettivamente costituire una misura di prevenzione efficace, ma solo a condizione che questa sia mirata e realizzata nel rispetto del diritto internazionale e nazionale e che persegua, inoltre, un effettivo scopo legittimo, così come inteso ai sensi dell'articolo 17 del Patto sui diritti civili e politici[98].

In ragione dell'accresciuta importanza del diritto alla privacy negli ultimi anni, nel 2015 il Consiglio per i diritti umani ha nominato, infine, il Professor Joseph Cannataci primo *Special Rapporteur per il diritto alla privacy*. Il mandato ha avuto una durata di tre anni e lo scopo di analizzare il diritto alla privacy nella sua evoluzione, con riferimento, soprattutto, ai recenti sviluppi tecnologici[99].

Nel primo rapporto, pubblicato il 24 novembre 2016[100], lo *Special Rapporteur* si è soffermato in particolare sul problema della sicurezza nazionale e delle implicazioni delle misure di sorveglianza sui diritti fondamentali. Nel rapporto viene infatti evidenziato come "[…] one of the most important issues in information policy and governance in the second decade of the twenty-first century deals with determining the *medio stat virtus* between, on the one hand, use of data for the benefit of society under the principles of Open Data and, on the other hand, the established principles we have developed to date with a view to protecting fundamental rights like privacy, autonomy and the free development of one's personality"[101]. Al riguardo, il Professor Canatacci non ritiene però utile affrontare la questione della tutela della privacy in termini di "privacy vs. security", bensì sarebbe più opportuno parlare di "privacy and security" "[…] since both privacy and security are

[97]Analogamente a quanto stabilito dall'articolo 8 CEDU, comma 2, secondo l'Alto Commissario le misure di sorveglianza devono essere: a) prescritte dalla legge; b) necessarie per perseguire uno scopo legittimo; c) proporzionate. Gli Stati dovrebbero, inoltre, adottare le suddette misure rispettando il principio di trasparenza e, in particolare, fornendo informazioni dettagliate circa lo scopo e la natura delle stesse.
[98]Consiglio per i diritti umani, *Report of the Office of the United Nations High Commissioner for Human Rights*, *The right to privacy in the digital age*, 27esima sessione, 30 giugno 2014, A/HRC/27/37, par. 24.
[99]Gli obiettivi specifici del mandato sono stabiliti dal Consiglio per i diritti umani con la risoluzione n. 28/16.
[100]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy,* 31esima sessione, 24 novembre 2016, A/HRC/31/64. Il.
[101]*Ibidem*, par. 1.

desiderata ... and both can be taken to be enabling rights rather than ends in themselves […]"[102].

Lo *Special Rapporteur*, infine, invita gli Stati a valutare un aggiornamento sia del Patto sui diritti civili e politici che della Convenzione del 1981 sul trattamento automatizzato dei dati personali, il quale tenga conto dello sviluppo economico e tecnologico avutosi nei diversi paesi nel mondo. Al fine di raggiungere il suddetto fine, è necessario "[…] establish a re-freshened understanding of what privacy means to different people in different places in different circumstances across the planet"[103].

Successivamente, nel 2017 viene pubblicato il secondo rapporto[104], avente ad oggetto l'analisi delle principali le problematiche connesse alla sorveglianza di massa e all'uso sempre più diffuso di *smartphones* e dispositivi elettronici. Questi ultimi, infatti, hanno accresciuto in maniera esponenziale la quantità di informazioni condivise dagli utenti, e allo stesso tempo, facilitato l'adozione di misure di interferenza da parte delle autorità nazionali[105].

Al riguardo, lo *Special Rapporteur* ribadisce l'importanza di condurre qualsiasi attività di sorveglianza sempre nel rispetto del diritto alla privacy[106], presa coscienza, però, anche delle difficoltà riscontrabili in questo contesto in ragione della mancanza di una chiara ed univoca definizione a livello internazionale di cosa debba intendersi per sorveglianza di massa e raccolta indiscriminata di informazioni[107]. Nel rapporto viene inoltre evidenziata l'inutilità di alcune misure di sorveglianza adottate, ad esempio, in Germania, le quali, discriminando tra i cittadini tedeschi ed europei e quelli non europei, non avevano tenuto in dovuta considerazione il fatto che, in realtà, la maggior parte degli attacchi terroristici avvenuti in Europa negli ultimi anni fossero stati posti in essere da persone nate e cresciute nel territorio europeo, e non dai cosiddetti "foreign fighters". In ragione di ciò, il Professor Cannataci ritiene che, anche in linea con quanto già stabilito a livello giurisprudenziale nel caso *Roman Zakharov*[108] deciso dalla Corte europea dei diritti umani e nel caso *Tele2*

[102]*Ibidem*, par. 24.
[103]*Ibidem*, par. 23.
[104]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, *Joseph. A. Cannataci*, 34esima sessione, 27 febbraio – 24 marzo 2017, A/HRC/34/60.
[105]*Ibidem, par. 23.*
[106]*Ibidem*, par. 29.
[107] *Ibidem,* par. 31.
[108]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit.

Sverige AB[109] deciso dalla Corte di giustizia, il criterio da adottare per decidere il soggetto destinatario della misura di sorveglianza debba essere essere quello del ragionevole sospetto e non, invece, quello della cittadinanza[110].

Infine, nell'ultimo rapporto del 28 febbraio 2018, viene fatto un riepilogo dell'attività svolta nei tre anni di mandato dallo *Special Rapporteur* e vengono identificati, inoltre, i principali ostacoli che ancora impediscono la piena ed effettiva tutela della privacy. Questi ultimi sono rappresentati, in particolare, dal "[…] lack or inadequacy of detailed rules, practical procedures and appropriate oversight mechanisms to ensure an independent, reliable and efficient control of surveillance, domestically and globally"[111].

1.6 LE DEROGHE AI DIRITTI UMANI IN SITUAZIONI DI EMERGENZA NAZIONALE

A volte gli Stati, al fine di tutelare la sicurezza nazionale, non si limitano ad adottare misure restrittive dei singoli diritti, ma fanno ricorso alla facoltà di deroga, laddove prevista, alle garanzie imposte nei trattati internazionali. É il caso ad esempio della Francia, la quale ha dichiarato, in seguito agli attacchi terroristi di novembre 2015, di volere ufficialmente derogare alla CEDU ai sensi dell'articolo 15 e all'articolo 4 del Patto sui diritti civili e politici, per tutelare la sicurezza dello Stato. Il Consiglio dei Ministri francese ha ufficializzato l'esercizio della facoltà di deroga temporanea alla Convenzione per tre mesi a causa della necessità di affrontare lo stato di emergenza del paese, poi prorogata per altri tre mesi. Pochi mesi prima, il 5 giugno 2015, anche l'Ucraina aveva dichiarato l'intenzione di volere derogare al Patto sui diritti civili e politici e alla CEDU. Secondo il governo Ucraino, la suddetta deroga si era resa necessaria al fine di assicurare i vitali interessi della società e dello Stato in risposta all'aggressione armata subita dalla Federazione Russa[112]. Per ultimo, il 21 luglio 2016 è stata notificata al Segretario generale

[109]Corte di giustizia (Grande Sezione), *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e altri*, sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15.
[110]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, *Joseph. A. Cannataci*, 34esima sessione, 27 febbraio – 24 marzo 2017, A/HRC/34/60, par. 44.
[111] Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, 37esima sessione, 26 febbraio-23 marzo 2018, A/HRC/37/62, par. 53.
[112]Notifica disponbile alla pagina: https://www.coe.int/en/web/secretary-general/news/-/asset_publisher/EYlBJNjXtA5U/content/ukraine-derogation-from-european-convention-on-human-rights/16695?inheritRedirect=false&redirect=http%3A%2F%2Fwww.coe.int%2Ffr%2Fweb%2Fsecretary-

del Consiglio d'Europa la dichiarazione ufficiale dell'esercizio della facoltà di deroga da parte delle autorità turche, terminata l'8 agosto 2018. Oltre agli appena citati casi, si possono identificare altri sei Stati membri della CEDU che hanno dichiarato di volere ricorrere all'articolo 15, ossia Albania, Armenia, Georgia, Grecia, Irlanda e Regno Unito.

Le pronunce più significative hanno riguardato l'esercizio della facoltà di deroga invocata dalla Grecia durante la "dittatura dei colonnelli" del 1967 - su cui la Corte europea dei diritti umani si è pronunciata nel cosiddetto caso Greco[113] - quella del Regno Unito dichiarata per fare fronte agli attacchi terroristici nell'Irlanda del Nord – da cui si sono originati i noti casi *Irlanda c. Regno Unito* e *Brannigan e McBride c. Regno Unito*[114]. Sempre il Regno Unito ha, inoltre, invocato la facoltà di deroga in seguito agli attacchi dell'11 settembre 2001, promulgando *l'Anti-terrorism, Crime and Security Act*, il quale ha di fatto esteso i poteri attribuiti alle pubbliche autorità per arrestare e detenere cittadini stranieri sospettati di minacciare la sicurezza nazionale o essere membri di associazioni terroristiche. Sulla compatibilità delle suddette misure con l'articolo 15 CEDU la Corte si è pronunciata con la sentenza *A. e altri c. Regno Unito*[115].

Degne di nota sono, infine, le due sentenze rese dalla Corte europea dei diritti umani con riferimento alle due deroghe invocate dalla Turchia, la prima nel 1990 per far fronte alla minaccia proveniente dall'organizzazione curda PKK, oggetto del caso *Aksoy c. Turchia*[116], e la seconda in seguito al colpo di stato di luglio 2016. Con riferimento a quest'ultima, i giudici di Strasburgo si sono pronunciati di recente con una sentenza resa il 20 marzo 2018[117] avente ad oggetto il ricorso presentato da due giornalisti, arrestati e detenuti per essere sospettati di fare parte del gruppo terroristico FETÖ/PDY ("Gülenist

---

general%2Fnews%3Fp_p_id%3D101_INSTANCE_EYlBJNjXtA5U%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D1

[113]Commissione europea dei diritti umani, *Danimarca, Norvegia, Svezia e Paesi Bassi c. Grecia* (il "caso Greco"), rapporto del 5 Novembre 1969, ricorsi nn. 3321/67 e altri.

[114]Corte europea dei diritti umani (Plenaria), *Brannigan e McBride c. Regno Unito,* sentenza del 26 maggio 1993, ricorsi nn. 14553/89 e 14554/89. Nel caso di specie, la Corte ha ritenuto che la minaccia terroristica dell'Irlanda del Nord rispecchiasse gli standard della pubblica emergenza, dal momento che essa aveva rappresentato per tanti anni una "particularly far-reaching and acute danger for the territorial integrity of the United Kingdom, the institutions of the six counties [of Northern Ireland] and the lives of the province's inhabitants" (par. 205).

[115]Corte europea dei diritti umani (GC), *A. e altri c. Regno Unito,* sentenza del 19 febbraio 2009, ricorso n. 3455/05. Il caso riguardava il ricorso presentato da undici cittadini stranieri che denunciavano di avere subito degli atti di tortura e di essere stati ingiustamente detenuti in carcere per un lasso di tempo eccessivo. La Corte stabiliva che le situazioni di emergenza pubblica minaccianti la sicurezza statale dovessero intendersi come del tutto eccezionali

[116]Corte europea dei diritti umani, *Aksoy c. Turchia*, sentenza del 18 dicembre 1996, ricorso n. n.100/1995/606/694.

[117]Corte europea dei diritti umani, *Şahin Alpay c. Turchia*, sentenza del 20 marzo 2018, ricorso n. 16538/17.

Terror Organisation/Parallel State Structure"), riconoscendo che il colpo di Stato ha costituito una seria minaccia alla vita e all'esistenza della nazione[118].

Le deroghe devono essere tenute distinte e non confuse con le limitazioni, come peraltro evidenziato anche nel *General Comment no. 29* del Comitato per i diritti umani relativo all'articolo 4 del Patto sui diritti civili e politici, nel quale si legge che "Derogation from some Covenant obligations in emergency situations is clearly distinct from restrictions or limitations allowed even in normal times under several provisions of the Covenant"[119]. Ciononostante, sia le deroghe che le limitazioni presentano quale elemento di comunione il fatto di dovere essere adottate nel rispetto del principio di proporzionalità.

Per quanto riguarda gli elementi di differenziazione si riscontra, innanzitutto, che, mentre le clausole di limitazione/restrizione sono previste, generalmente al secondo comma, nella medesima disposizione che tutela il diritto suscettibile di restrizione, le deroghe sono invece disciplinate in specifiche fonti normative, rappresentate nel sistema di tutela internazionale dei diritti umani oggetto di analisi del presente elaborato rispettivamente dall'articolo 4 del Patto sui diritti civili e politici e dall'articolo 15 CEDU. Dal punto di vista sostanziale, inoltre, "le prime possono essere definite, con una certa approssimazione, come quelle limitazioni al godimento di singoli diritti, corrispondenti in buona sostanza alle libertà civili e politiche della tradizione democratica occidentale, suscettibili di essere arrecate in presenza di determinate ragioni di interese pubblico e nel rispetto di certe condizioni. Per deroga si intende invece la facoltà concessa agli Stati in alcuni strumenti internazionali di sospendere la garanzia dei diritti in essi previsti, ad eccezione di alcuni, quando ciò si dimostri necessario per far fronte a situazioni di particolari difficoltà per lo Stato"[120].

Data la natura del tutto eccezionale della deroga, solo in pochi casi gli Stati hanno fatto ricorso ad essa e, conseguentemente, altrettanto poche sono le pronunce e i pareri resi dai relativi organi internazionali di controllo. Per quanto riguarda il sistema del Patto sui diritti civili e politici, il Comitato per i diritti umani si è pronunciato solo poche volte, tra

[118] *Ibidem*, par. 64.
[119] Comitato per i diritti umani, *CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency*, 31 agosto 2001, UN Doc CCPR/C/21/Rev1/Add11, par. 4.
[120] Cfr. I. VIARENGO, *Deroghe e restrizioni alla tutela dei diritti umani nei sistemi internazionali di garanzia*, in *Rivista di diritto internazionale*, 2005, pag. 955.

cui si ricorda, oltre al già precedentemente citato *General Comment no. 29*[121], un *General Comment* del 1992 relativo ad un rapporto presentato dalla Tanzania[122]. In quest'ultimo documento, in particolare, l'organo delle Nazioni Unite aveva specificato che le misure di deroga dovessero essere intese come limitate "to the extent strictly required by the exigencies of the situation"[123].

Sempre dal punto di vista procedurale, gli Stati hanno inoltre l'obbligo di giustificare non solo la dichiarazione pubblica di emergenza nazionale, ma anche tutti gli atti adottati in base ad essa. I casi in cui è generalmente possibile invocare l'esercizio della facoltà di deroga sono le catastrofi naturali, le dimostrazioni di massa violente, gli incidenti industriali.

A livello normativo, l'articolo 4 del Patto sui diritti civili e politici prevede che "In caso di pericolo pubblico eccezionale, che minacci l'esistenza della nazione e venga proclamato con atto ufficiale, gli Stati parti del presente Patto possono prendere misure le quali deroghino agli obblighi imposti dal presente Patto, nei limiti in cui la situazione strettamente lo esiga, e purché tali misure non siano incompatibili con gli altri obblighi imposti agli Stati medesimi dal diritto internazionale e non comportino una discriminazione fondata unicamente sulla razza, sul colore, sul sesso, sulla lingua, sulla religione o sull'origine sociale". Al secondo comma vengono indicati, invece, i diritti che non possono essere in alcun modo derogati, ossia il diritto alla vita (art. 6), il divieto di tortura e trattamenti inumani e degradanti (art. 7), il divieto di schiavitù (art. 8, parr. 1 e 2), la detenzione arbitraria (art. 11), il principio di irretroattività della legge penale (art. 15), il risconoscimento della personalità giuridica e, infine, il diritto alla libertà di pensiero, coscienza e religione. A ciò si aggiunga anche il principio di non discriminazione, il quale, pur non essendo espressamente elencato dalla Convenzione tra i diritti inderogabili, ha assunto valore di limite generale alla possibilità di ricorrere all'esercizio della facoltà di deroga da parte delle autorità statali[124]. Inoltre, in base a quanto previsto nel *General Comment no. 29* del Comitato per i diritti umani, nell'articolo 4, par. 2, andrebbero inclusi anche il diritto delle persone detenute ad un trattamento dignitoso, il divieto di presa di

[121]Comitato per i diritti umani, *CCPR General Comment No. 29: Article 4: Derogations during a State of Emergency*, 31 agosto 2001, CCPR/C/21/Rev1/Add11.
[122]Comitato per i diritti umani, *Comments on the United Republic of Tanzania*, 28 dicembre 1992, CCPR/C/79/Add.12.
[123]*Ibidem,* par. 59.
[124]Cfr. I. VIARENGO, *op. cit.*, v. sopra nota 120, pag. 975.

ostaggi, trasferimenti e detenzioni arbitrarie, l'incitamento alla guerra, all'odio razziale e religioso, nonché il divieto di genocidio[125].

Un'analoga disposizione è prevista anche dalla CEDU, la quale si differenzia dal Patto sui diritti civili e politici solo sotto il profilo dei diritti non derogabili, rappresentati dal diritto alla vita (art. 2) – salvo i casi di decesso causato da atti legittimi di guerra – il divieto di tortura e trattamenti inumani e degradanti (art. 3), il divieto di schiavitù (art. 4, par. 1) e il principio *nulla poena sine lege* (art. 7). In realtà, nel caso *A. e altri c. Regno Unito* risalente al 2009[126], la Corte europea dei diritti umani aveva messo in evidenza le ulteriori differenze esistenti tra i due tipi di deroga, stabilendo che "While the United Nations Human Rights Committee has observed that measures derogating from the provisions of the ICCPR must be of "an exceptional and temporary nature" the Court's case-law has never, to date, explicitly incorporated the requirement that the emergency be temporary, although the question of the proportionality of the response may be linked to the duration of the emergency […]"[127]. Nel caso di specie, in particolare, la situazione di minaccia alla pubblica sicurezza, causata dai movimenti terroristi sviluppatesi nel nord dell'Irlanda, avrebbe potuto continuare per diversi anni.

Dal punto di vista sostanziale, la deroga può essere invocata solo a tre condizioni: deve sussistere una guerra o un'emergenza pubblica che minacci la vita della nazione, le misure adottate devono essere strettamente necessarie e compatibili con gli obblighi previsti dal diritto internazionale. Orbene, mentre il requisito della sussistenza dello stato di guerra non ha dato origine a particolari problemi interpretativi, potendosi rinvenire tutte le volte in cui uno Stato dichiara o riceve una dichiarazione ufficiale di guerra o si trova coinvolto in un conflitto armato, gli altri elementi contenuti nell'articolo 15 CEDU meritano, invece, una più attenta trattazione[128].

Per quanto riguarda, innanzitutto, il primo requisito, la Corte europea dei diritti umani ha specificato nel caso *Lawless c. Irlanda (n.3)* che per pubblica emergenza debba intendersi "[…] an exeptional situation of crisis or emergency which affects the whole population and constitutes a threat to the organized life of the community of which the

[125]Comitato per i diritti umani, *General Comment no. 29: Article 4: Derogations during a State of Emergency*, 31 agosto 2001, CCPR/C/21/Rev1/Add11cit., parr. 12 e 13.
[126]Corte europea dei diritti umani (GC), *A. e altri c. Regno Unito,* cit.
[127]Corte europea dei diritti umani (GC), *A. e altri c. Regno Unito,* cit., par. 178.
[128]Cfr. Y. ARAI-TAKANASHI e altri, *Theory and Practise of the European Convention on Human Rights*, Intersentia, Cambridge 2006, pag. 1059.

State is composed"[129]. Nel caso di specie, in particolare, la situazione di emergenza era stata dedotta da alcuni elementi, come l'occupazione del territorio irlandese da parte di eserciti segreti che svolgevano attività anticostituzionali e facevano ricorso alla forza per raggiungere i propri scopi e l'incremento della minaccia terroristica tra il 1956 e il 1957. In ogni caso, viene generalmente lasciato agli Stati un ampio margine di apprezzamento nel decidere se sussiste una situazione di emergenza tale da giustificare una deroga all'articolo 15[130].

In secondo luogo, le misure adottate dallo Stato devono essere strettamente necessarie. A tal riguardo, la Corte europea dei diritti umani ha ritenuto di dovere valutare e tenere in considerazione diversi elementi, tra cui il fatto che la legge possa essere sufficientemente adeguata al fine di far fronte al pericolo pubblico[131], che le misure costituiscano una risposta adeguata alla situazione di emergenza[132], siano utilizzate per gli scopi per cui erano state adottate[133] e siano, infine, soggette a controllo o revisione contro eventuali abusi da parte delle autorità pubbliche[134]. Occorre inoltre che le misure siano proporzionate ai fini perseguiti[135]. Secondo i giudici di Strasburgo, infatti, nonostante sia compito degli Stati decidere la sussistenza o meno di un'emergenza nazionale – trovandosi in una condizione migliore rispetto a quella dei giudici internazionali – essi non godono di un margine di apprezzamento illimitato, ma questo deve sempre essere soggetto allo scrutinio della Corte.

Infine, le misure di deroga adottate devono essere compatibili con gli altri obblighi derivanti dal diritto internazionale e non comportare alcuna discriminazione fondata sulla razza, colore, sesso, lingua, religione e origine sociale. Ad esempio, nel caso *Brannigan e McBride c. Regno Unito* i ricorrenti sostenevano che il Regno Unito, non dichiarando pubblicamente lo stato di emergenza nazionale, così come richiesto dall'articolo 4 del Patto sui diritti civili e politici, si fosse reso inadempiente nei confronti del suddetto

[129]Corte europea dei diritti umani, *Lawless c. Irlanda (n. 3),* sentenza del 1 luglio 1961, ricorso n. 332/57, par. 28.
[130]Corte europea dei diritti umani (Plenaria), *Brannigan e McBride c. Regno Unito*, cit., par. 207.
[131]Corte europea dei diritti umani, *Lawless c. Irlanda (n. 3),* cit., par. 36*;* Corte europea dei diritti umani (Plenaria), *Irlanda c. Regno Unito*, sentenza del 18 gennaio 1978, ricorso n. 5310/71, par. 212.
[132]Corte europea dei diritti umani (Plenaria), *Brannigan e McBride c. Regno Unito*, cit., par. 51.
[133]Corte europea dei diritti umani, *Lawless c. Irlanda (n. 3),* cit., par. 38.
[134]Corte europea dei diritti umani, *Lawless v. Ireland (no. 3),* cit., par. 37; Corte europea dei diritti umani (Plenaria) *Brannigan e McBride c. Regno Unito*, cit., parr. 61-65; Corte europea dei diritti umani, *Aksoy c. Turkey*, cit., parr. 79-84.
[135]Corte europea dei diritti umani (GC), *A. e altri c. Regno Unito*, cit. par.190

obbligo internazionale[136]. A tal riguardo, la Corte europea dei diritti umani riteneva che, nonostante non fosse suo compito definire cosa si intendesse con la locuzione "proclamato con atto ufficiale" in base all'articolo 4, par. 1, del Patto, essa dovesse comunque valutare la fondatezza della tesi sostenuta dai ricorrenti. Nel caso di specie, in particolare, la dichiarazione del 22 dicembre 1988 del Segretario di Stato rivolta alla Camera dei Comuni poteva senz'altro essere considerata una proclamazione pubblica di deroga. Conseguentemente, non veniva ravvisata alcuna violazione della CEDU[137].

La sussistenza di una dichiarazione pubblica di esercizio della facoltà deroga da parte dello Stato, la quale deve essere notificata, unitamente alle altre eventuali misure adottate, rispettivamente al Segretario generale del Consiglio d'Europa e al Segretario generale delle Nazioni Unite[138], costituisce, allo stesso tempo, anche il principale requisito di natura procedurale, previsto dall'articolo 15, par. 3, CEDU e dall'articolo 4, par. 3 del Patto internazionale sui diritti civili e politici. La dichiarazione pubblica deve inoltre indicare il termine massimo di durata della deroga e i motivi che l'hanno ispirata[139].

Per ragioni di completezza pare opportuno ricordare che la possibilità di invocare la deroga è prevista, oltre che nei già citati sistemi di tutela previsti dal Patto sui diritti civili e politici e dalla CEDU, anche dalla Convenzione americana sui diritti umani[140]. L'articolo 27 della norma in esame prevede, infatti, che in caso di guerra, pericolo pubblico o altra emergenza che minacci l'indipendenza o la sicurezza di uno Stato membro, quest'ultimo possa adottare delle misure di deroga ai diritti e agli obblighi imposti dalla Convenzione, nell'estensione e per il periodo di tempo strettamente richiesti dalle contingenze, a condizione che dette misure non siano incompatibili con altri obblighi che lo Stato ha assunto in base al diritto internazionale e non comportino discriminazioni sulla base di razza, colore, sesso, lingua, religione o origine sociale. Inoltre, alla pari di quanto previsto dal Patto sui diritti civili e politici e dalla CEDU, al secondo comma vengono elencati i

[136]Corte europea dei diritti umani (Plenaria), *Brannigan e McBride c. Regno Unito,* cit., par. 68.
[137]*Ibidem*, cit., parr. 72 e 73.
[138]Cfr. C. FOCARELLI, *op. cit.*, vedi sopra nota 61, pag. 259.
[139]Sul punto cfr. i seguenti casi della Corte europea dei diritti umani: Commissione europea dei diritti umani, *Cipro c. Turchia*, rapporto del 4 ottobre 1983, ricorso n. 8007/77; Commissione europea dei diritti umani, *Grecia c. Regno* Unito, rapporto del 26 settembre 1958, ricorso n. 176/56; Corte europea dei diritti umani, *Lawless c. Irlanda*, cit., Corte europea dei diritti umani, *Aksoy c. Turchia,* cit.; Corte europea dei diritti umani, *Brogan e altri c. Regno Unito*, sentenza del 29 novembre 1988, ricorsi nn. 11209/84 e altri.
[140]Convenzione americana sui diritti umani, adottata dall'Organizzazione degli Stati Americani (OAS) il 21 novembre 1969 a San José di Costarica ed entrata in vigore il 18 luglio 1978. Per contro, nulla è previsto a riguardo nella Convenzione sui diritti dell'Infanzia.

diritti inderogabili, ossia il diritto alla personalità giuridica (articolo 3); il diritto alla vita (articolo 4); il diritto ai trattamenti umani (articolo 5) e il divieto di schiavitù (articolo 6); l'irretroattività della legge penale (articolo 9); la libertà di coscienza e religione (articolo 12); i diritti della famiglia e il diritto al nome (articoli 17 e 18); il diritto alla nazionalità (articolo 20) e, infine, i diritti di partecipazione politica (articolo 23).

A differenza del Patto sui diritti civili e politici e della CEDU, i quali indicano come condizione per invocare l'esercizio della facoltà di deroga la sussistenza di una pubblica emergenza che minacci la "vita della nazione", la Convenzione americana sui diritti umani prevede, invece, una formula più generica, invocando la minaccia "all'indipendenza e alla sicurezza di uno Stato". Per quanto riguarda le condizioni procedurali, in maniera analoga al Patto e alla CEDU, è previsto che lo Stato notifichi al Segretario generale dell'Organizzazione degli Stati Americani quali disposizioni della Convenzione intende sospendere, nonché le ragioni che hanno motivato l'esercizio della facoltà di deroga e la data in cui essa dovrà cessare.

In conclusione, si può ritenere che sia le deroghe – analizzata nel presente paragrafo – sia le restrizioni ai diritti umani, che costituiranno oggetto di trattazione nel prossimo capitolo, rappresentano entrambe due strumenti per bilanciare, da un lato, i diritti degli individui e, dall'altro lato, le esigenze della collettività di un determinato Stato, rappresentate, per esempio, dalla sicurezza nazionale, dai bisogni di natura economica o ambientale. A livello generale, infatti, la possibilità di restringere le tutele offerte ai singoli dai sistemi internazionali e statali di tutela dei diritti umani trova il suo riferimento normativo nell'articolo 29, par. 2, della Dichiarazione universale dei diritti, a menzione del quale "Nell'esercizio dei suoi diritti e delle sue libertà, ognuno deve essere sottoposto soltanto a quelle limitazioni che sono stabilite dalla legge per assicurare il riconoscimento e il rispetto dei diritti e delle libertà degli altri e per soddisfare le giuste esigenze della morale, dell'ordine pubblico e del benessere generale in una società democratica[…]".

CAPITOLO 2
IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI NEI SISTEMI REGIONALI DI TUTELA DEI DIRITTI UMANI

2.1 LA TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA 2.1.1 Le fonti europee di natura primaria 2.1.1.1 La clausola di limitazione ex art. 52 della Carta dei diritti fondamentali dell'Unione europea 2.1.2 Le fonti europee di natura secondaria 2.1.2.1 Il regolamento (UE) 2016/679 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) 2.1.2.1.1 La clausola di limitazione nel regolamento (UE) 2016/679. 2.1.2.2 La direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati 2.1.2.2.1 La clausole di limitazione nella direttiva (UE) 2016/680 2.1.2.3 La direttiva 2016/681 sull'uso dei dati del codice di prenotazione (PNR) ai fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e reati gravi 2.1.2.4 La proposta di regolamento *e-privacy* 2.1.2.4.1 La clausola di limitazione nella proposta di regolamento *e-privacy* 2.2 LA TUTELA DEI DATI PERSONALI NEL SISTEMA REGIONALE DEL CONSIGLIO D'EUROPA 2.2.1 L'articolo 8 CEDU. 2.2.1.1 Le limitazioni all'articolo 8 CEDU 2.2.2 La Convenzione 108 del Consiglio d'Europa 2.2.3 La Raccomandazione R. (87) regolante l'utilizzo dei dati personali nel settore di polizia 2.3 LA CONVENZIONE AMERICANA SUI DIRITTI UMANI E LA CARTA ARABA DEI DIRITTI UMANI.

2.1 LA TUTELA DEI DATI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA

2.1.1 Le fonti europee di natura primaria

Le istituzioni europee, dell'allora Comunità europea, hanno iniziato ad interessarsi al problema della protezione dei dati personali a partire dagli anni '80 del XX secolo, quando la Commissione europea in una raccomandazione del 1981 sollecitava gli Stati membri a ratificare la Convenzione 108 del Consiglio d'Europa[141], in modo da armonizzare le normative nazionali e favore un mercato comune anche nel settore delle informazioni[142].
Ad oggi, il suddetto diritto trova innanzitutto protezione nelle fonti primarie del diritto dell'Unione europea, ossia nei Trattati. Esso è stato introdotto per la prima volta nel Trattato di Amsterdam, il quale prevedeva all'articolo 286 TCE, paragrafo 1, che "A decorrere dal 1° gennaio 1999 gli atti comunitari sulla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati si applicano alle istituzioni e agli organismi istituiti dal presente trattato o sulla base del medesimo".

Ma è grazie al Trattato di Lisbona che la tutela dei dati personali è stato riconosciuta come un principio fondamentale europeo. L'Unione europea ha infatti, grazie all'articolo 16 TFUE (già articolo 286 TCE), la specifica competenza a tutelare, tramite atti legislativi

[141]Consiglio d'Europa, *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, Strasbourg, 28.I.1981 ,Série des traités européens - n° 108.
[142]Cfr. F. MARTINES, *op. cit.*, v. sopra nota 46, pag. 725.

adottati con procedura legislativa ordinaria e soggetti al controllo di autorità indipendenti, i dati personali degli individui[143]. Per la tutela dei suddetti diritti l'Unione europea può inoltre ricorrere, se necessario, alla Corte di giustizia. L'articolo 8 della Carta dei diritti fondamentali dell'Unione europea che ha assunto, grazie alla previsione normativa contenuta nel nuovo articolo 6, c. 1, TUE[144], lo stesso valore giuridico dei Trattati, prevede che:

> "1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano.
>
> 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica.
>
> 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente"[145].

Sul punto occorre sottolineare che la Carta dei diritti fondamentali dell'Unione europea è, ad oggi, ancora l'unico strumento di tutela dei diritti umani a distinguere espressamente tra il diritto alla privacy, sancito all'articolo 7[146], e il diritto alla protezione dei dati personali.
Al pari di quanto già previsto a livello internazionale, si può affermare che anche nel sistema giuridico europeo il diritto alla protezione dei dati personali imponga non solo obblighi negativi – ricavabili *a contrarii* dall'articolo 8, par. 2 – ma anche obblighi positivi[147]. Con riferimento a questi ultimi, infatti, l'articolo 16, par. 2, TFUE, stabilisce

---

[143]Articolo 16 TFUE "Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea".
[144]Articolo 6, par. 1, TUE "L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati".
[145]Non è ancora chiaro se la Carta abbia anche effetti orizzontali – ossia che disciplini anche i rapporti tra due soggetti privati o fra una pubblica autorità e un soggetto privato – ma si tende a propendere per la soluzione negativa. Questa lacuna potrebbe dare origine a *deficit* di tutela dei diritti degli individui, nella misura in cui la Carta non è applicabile, ad esempio, alle grandi società che raccolgono quotidianamente enormi quantità di informazioni personali. Cfr. H. HIJMANS, *op. cit.*, v. sopra nota 56, pag. 36.
[146]Articolo 7 Carta dei diritti fondamentali dell'Unione europea "Ogni individuo ha il diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle proprie comunicazioni".
[147]Cfr. H. HIJMANS, *op. cit.*, v. sopra nota 56, pag. 48.

che: “Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti”.

2.1.1.1 La clausola di limitazione ex art. 52 Carta dei diritti fondamentali dell’Unione europea

L’articolo 8 della Carta dei diritti fondamentali dell’Unione europea non contiene espressamente alcuna clausola di limitazione. Essa può però ricavarsi in maniera indiretta dall’articolo 52, che disciplina in generale tutte le limitazioni ai diritti tutelati dalla Carta. In particolare, ivi viene disposto che “1. Eventuali limitazioni all’esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall’Unione o all’esigenza di proteggere i diritti e le libertà altrui. 2. I diritti riconosciuti dalla presente Carta che trovano fondamento nei trattati comunitari o nel trattato sull’Unione europea si esercitano alle condizioni e nei limiti definiti dai trattati stessi. 3. Laddove la presente Carta contenga diritti corrispondenti a quelli garantiti dalla CEDU, il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta convenzione. La presente disposizione non preclude che il diritto dell’Unione conceda una protezione più estesa”.

In base a quanto previsto dalla norma, si ricava, innanzitutto, che diritto dell’Unione europea può, in linea con quanto generalmente stabilito in materia di diritti umani, restringere il diritto alla protezione dei dati solo adottando misure che necessarie e proporzionate. In secondo luogo, in base al comma 3, è necessario tenere in considerazione, nel caso in cui sorgano problemi relativi al bilanciamento dei diritti, sia dei principi enunciati dalla Carta di Nizza, sia di quelli enunciati dalla CEDU[148] - inclusi, con

[148]Cfr. F. PIZZETTI, *op. cit.*, vedi sopra nota 45, pag. 143-144.

riferimento quest'ultima fonte, anche i principi sanciti dalla relativa giurisprudenza della Corte europea dei diritti umani.

2.1.2 Le fonti europee di natura secondaria

Sempre a livello europeo, i dati personali vengono disciplinati anche da alcune fonti legislative di natura secondaria adottate soprattutto nel corso degli ultimi anni, tra cui rilevano, in particolare, la direttiva 95/45/CE – che ha costituito per anni il testo di riferimento in materia di protezione dei dati personali nell'Unione europea e sostituita ora dal regolamento (UE) 2016/679[149] - la direttiva 2002/58/CE (la c.d. direttiva *e-Privacy*, invalidata con la sentenza della Corte di giustizia nel caso *Tele2 Sverige AB*[150]), il regolamento 2001/45/CE 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 e la direttiva 2006/24/CE (la c.d. *Data Retention Directive*, invalidata, invece, nel caso *Digital Rights Ltd*[151]). In questo ambito assumono inoltre rilevanza la decisione quadro 2008/977/GAI del Consiglio del 27 novembre 2008 sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, sostituita ora dalla direttiva (UE) 2016/680 e, infine, la direttiva 2009/136/CE "recante modifiche della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e servizi di comunicazione elettronica".

Per ragioni connesse all'oggetto di indagine verranno analizzate, seppur soltanto in termini generali data l'ampiezza e la complessità dell'apparato legislativo europeo, il regolamento europeo (UE) 2016/679 e la direttiva (UE) 2016/680 facenti parte del nuovo "Pacchetto protezione dati", nonché la nuova proposta di regolamento relativo alle comunicazioni elettroniche. Infine, verranno messe brevemente in evidenza le più importanti novità introdotte dalla direttiva (UE) 2016/681 ("direttiva PNR") in materia di trasporti aerei, la cui disciplina è stata fortemente influenzata dalle nuove politiche dell'Unione europea in materia di contrasto al terrorismo internazionale e di *law*

[149]Cfr. N. CATELAN, S. CIMAMONTI, J.B. PERRIER, *La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne,* Presses Universitaire d'Aix- Marseille, 2014, pag. 129. Cfr. F. BIGNAMI, *Privacy and Law Enforcement in the European Union: The Data Retention Directive,* in *Chicago Journal of International Law*, 2007.
[150]Corte di giustizia (Grande Sezione), *Tele2 Sverige AB,* cit.
[151]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd,* cit.

enforcement.

Per quanto riguarda, innanzitutto, il nuovo "Pacchetto protezione dati" si rileva, in via preliminare, che le due fonti normative forniscono, rispettivamente agli articoli 4(1) e 3(1), una definizione comune di dato personale, più ampia rispetto alla precedente normativa[152]. In particolare, viene definito dato personale "qualsiasi informazione riguardante una persona fisica identificata o identificabile, (l'«interessato»), si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici dell'identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale di tale persona fisica". Dalla lettura della norma si ricava, infatti, che la nuova nozione ricomprende anche l'identificativo *online*.

Inoltre, le due fonti normative, pur disciplinando ambiti di competenza completamente diversi, hanno in comune diversi principi ispiratori e questo costituisce un chiaro segno dell'intento del legislatore europeo di cercare di uniformare, nel miglior modo possibile, l'intera disciplina in materia di protezione dei dati personali.

Questi principi, sanciti rispettivamente all'articolo 5 del regolamento (UE) 2016/679 e dall'articolo 4 della direttiva (UE) 2016/680, sono:

- Liceità, correttezza e trasparenza
- Limitazione della finalità (del trattamento): i dati devono essere raccolti solo per finalità determinate, esplicite e legittime, ed essere successivamente utilizzati in modo conforme alle suddette finalità;
- Minimizzazione dei dati: i dati devono essere adeguati e limitati nei limiti della finalità del loro trattamento;
- Esattezza;
- Limitazione della conservazione: i dati devono essere conservati per un tempo non superiore a quanto necessario alle finalità per le quali sono trattati, salvo che siano per

[152]Articolo 2, lettera a) decisione quadro 2008/977/GAI del Consiglio "«dati personali» qualsiasi informazione concernente una persona fisica identificata o identificabile («persona interessata»); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un numero di identificazione o a uno o più elementi caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale. La stessa definizione è presente nell'articolo 2, lettera a) della direttiva 95/46/CE.

finalità di interesse pubblico, di ricerca scientifica o storica o fini statistici;

- Integrità e riservatezza: i dati devono essere trattati in maniera sicura e devono essere adottate tutte le misure necessarie al fine di evitare danni causati da trattamenti non autorizzati o illeciti, o dalla perdita dei dati;

Oltre ai principi appena menzionati, vengono in rilievo anche altre importanti novità introdotte dal regolamento e dalla direttiva e comuni ad entrambe le fonti normative. Tra queste assume una particolare importanza, ai fini della presente indagine, il cosiddetto *Data Breach*.

Si constata inoltre che, al pari delle altre fonti del diritto precedentemente analizzate, emerge anche in questa sede la natura relativa della tutela dei dati personali. Il considerando n. 4 del regolamento (UE) 2016/679 stabilisce infatti che "Il trattamento dei dati personali dovrebbe essere al servizio dell'uomo. Il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità […]". Gli Stati possono, infatti, derogare alla tutela riconosciuta dalle suddette disposizioni normative attraverso specifiche modalità e finalità stabilite dalle stesse clausole di limitazione, sempre nel rispetto però delle tutele sancite in materia dalla Carta dei diritti fondamentali dell'Unione europea e dalla CEDU, nonché dalle relative giurisprudenze della Corte di giustizia e della Corte europea dei diritti umani[153].

Infine, sia il regolamento (UE) 2016/679 che la direttiva (UE) 2016/680 non si applicano al trattamento dei dati personali nell'ambito della sicurezza nazionale, che resta prerogativa degli Stati[154]. Invero, nonostante l'Unione europea abbia tentato negli ultimi anni di adottare diverse misure legislative volte ad armonizzare le fonti nazionali in materia di politica estera e difesa comune, la sicurezza resta una competenza esclusiva statale[155]. In merito viene inoltre in rilievo l'articolo. 4 co. 2, TUE, a menzione del quale l'Unione "rispetta [...] l'identità nazionale [degli Stati membri] insita nella loro struttura fondamentale, politica e costituzionale [...] e le funzioni dello Stato [...] di mantenimento

[153]Considerando 46 direttiva (UE) 2016/680.
[154]Considerando 16 regolamento (UE) 2016/679; considerando 14 direttiva (UE) 2016/680.
[155]Cfr. P.-Y MONJAL, *Les dossier européens: actualités en bref, Protection des données à caractère personnel (la protection des personnes physiques à l'égard du traitement des données à caractère personnel : le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016,* in *Revue du droit de l'Union européenne* 2016, pag. 634.

dell'ordine pubblico e di tutela della sicurezza nazionale. In particolare, la sicurezza nazionale resta di esclusiva competenza di ciascuno Stato membro".

2.1.2.1 Il regolamento (UE) 2016/679 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)

La direttiva 95/46/CE è stata ora sostituita dal nuovo regolamento (UE) 2016/679, pubblicato il 4 maggio 2016 sulla Gazzetta ufficiale dell'Unione europea e parte integrante, come già precedentemente anticipato, insieme alla direttiva (UE) 2016/680 del cosiddetto "Pacchetto protezione dati". Il regolamento e la direttiva saranno direttamente applicabili in tutti Paesi membri UE a partire dal 25 maggio 2018.

Il regolamento subentrerà alla precedente direttiva 95/46/CE[156], la quale era stata concepita in un momento in cui una piccolissima parte della popolazione europea utilizzava Internet, non esistevano ancora i *social network*, né tanto meno i problemi legati alla sorveglianza di massa. La nuova regolamentazione si è resa necessaria in ragione della crescente importanza economica assunta dai dati personali nel contesto europeo, dal momento che, così come evidenziato dal considerando 5, "L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese […]".

Inoltre, in base a quanto previsto dal considerando n. 2, il regolamento ha lo scopo di contribuire alla realizzazione di uno spazio di libertà, sicurezza e giustizia e di un'unione economica che porti alla convergenza delle economie nel mercato interno e al benessere delle persone fisiche.

La nuova disciplina europea ha introdotto importanti novità, che garantiscono una maggiore tutela degli individui, tra cui, in particolare, la portabilità dei dati, l'estesa

[156]La direttiva 95/46/CE rappresenta la prima fonte di natura secondaria in materia di protezione dei dati personali adottata dall'Unione europea. Essa aveva il duplice obiettivo di promuovere, da un lato, il mercato interno dei dati personali attraverso la libera circolazione delle informazioni e, dall'altro lato, di proteggere i diritti degli individui (considerando n. 3).

applicazione territoriale[157], la figura del "Data Protection Officer", il diritto di accesso ai dati, nuove regole per la trasparenza dei dati e il concetto "Privacy by Design".

Tra le più importanti novità introdotte dal nuovo regolamento vi è inoltre l'obbligo, facente capo al titolare del trattamento e al responsabile del trattamento, di notificare la violazione dei dati personali ai sensi degli articoli 33 e 34[158]. L'articolo 4 del regolamento definisce violazione dei dati personali "la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Ai sensi dell'articolo 33, il titolare del trattamento[159] ha l'obbligo di notificare la violazione dei dati personali all'autorità competente ai sensi dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, essa deve essere corredata dai motivi del ritardo". Il responsabile del trattamento[160] ha, invece, l'obbligo di notificare la violazione al titolare, in modo che questi possa procedere agli adempimenti previsti dal primo comma.

La notifica deve indicare, almeno, la natura della violazione e il numero approssimativo dei soggetti interessati dalla stessa (a), il nome e i dati del responsabile della protezione dei

[157]Articolo 3 regolamento (UE) 2016/679 "1.Il presente regolamento si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento dell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione. 2. Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano: a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione. 3. Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico".

[158]Il cosiddetto "Data Breach", di origine statunitense e presente ora anche in diversi Paesi del Sud-est asiatico, non è una realtà del tutto nuovo anche nel panorama europeo: esso era infatti già previsto nella direttiva 2002/58/CE relativa alle comunicazioni elettroniche. Cfr. F. PIZZETTI, *op. cit.*, v. sopra nota 45, pagg. 290 e ss.

[159]Il titolare del trattamento viene definito all'articolo 4, par. 1, regolamento (UE) 2016/679 come "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali"; il responsabile del trattamento è, invece, "la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento".

[160]I termini "titolare del trattamento" e "responsabile del Trattamento" erano già presenti nel codice italiano sulla protezione dei dati personali. Il mantenimento di entrambe le diciture all'interno del nuovo regolamento è stato fortemente caldeggiato dalle autorità italiane in sede di discussione legislativa al fine di evitare problemi interpretativi – che avrebbero comportato nuovi costi – in capo alle società e ai professionisti che già si occupavano di dati personali.

dati, o di un altro soggetto cui chiedere informazioni (b), le possibili conseguenze della violazione (c), le misure adottate o che il titolare del trattamento intende adottare al fine di porre rimedio alla violazione dei dati personali (d). L'articolo 34 della direttiva (UE) 2016/680 prevede anche l'ipotesi in cui la notifica debba essere effettuata direttamente all'interessato, ossia quando la violazione possa "presentare un rischio elevato per i diritti e le libertà delle persone fisiche […].

Il regolamento (UE) 2016/679, che per sua natura è direttamente applicabile all'interno degli Stati membri, comporterà importanti obblighi di adattamento fra le diverse normative statali in tema di protezione dei dati personali. Per quanto riguarda, infatti, l'appena esposto *Data Breach*, nella maggior parte degli Stati membri non esiste un obbligo di notifica, o, anche quando tale obbligo sussiste, le sanzioni previste in caso di violazione sono minime. In realtà alcuni Paesi, tra cui l'Italia e la Germania, avevano introdotto l'obbligo di notifica anche prima dell'approvazione del regolamento europeo. Per quanto riguarda la Germania, quest'obbligo è stato inserito nel settembre 2009 nella sezione 42a dell'emendato Codice Federale in materia di protezione dei dati personali (BDSG)[161]. In Italia, il Decreto Legislativo no. 69/2012 ha emendato il codice Privacy e ha previsto nuovi obblighi di notifica al Garante della Privacy in caso di violazione dei dati personali in caso di comunicazioni elettroniche.

Si ricordi, infine, che la disciplina in esame ha introdotto i principi di necessità, proporzionalità e legittimità – derivanti dalla normativa e dalla giurisprudenza relativa all'articolo 8 CEDU – non previsti, invece, nella precedente direttiva 95/46/CE.

[161]Cfr. A. FREIHERR VON DEM BUSSCHE, M. STAMM, *Data Protection in Germany,* Verlag C.H. Beck, Monaco 2013, pag. 20.

2.1.2.1.1 La clausola di limitazione nel regolamento (UE) 2016/680

L'articolo 23 prevede la facoltà in capo all'Unione europea, o allo Stato membro cui è soggetto il titolare o il responsabile del trattamento, di limitare mediante misure legislative la portata dei diritti e degli obblighi derivanti dal regolamento, qualora le suddette limitazioni siano necessarie a salvaguardare la sicurezza nazionale, la difesa e la sicurezza pubblica, oppure al fine di prevenire, indagare e perseguire reati od eseguire sanzioni penali. La facoltà di limitare gli obblighi e i diritti previsti dal regolamento era, in realtà, già prevista dall'articolo 13 dell'ora abrogata direttiva 95/46/CE[162]. Rispetto alla precedente disciplina, però, gli elementi innovativi sono rappresentati dalle serie di ulteriori tutele che la misura legislativa di deroga deve fornire al cosiddetto *data subject* e dal fatto che le limitazioni devono essere *necessarie* e *proporzionate*. Questi ultimi principi sono il frutto dell'influenza della giurisprudenza della Corte europea dei diritti umani sul diritto dell'Unione europea e rappresentano una trasposizione all'interno dello stesso dei criteri fondanti l'articolo 8, comma 2, della CEDU.

Per quanto riguarda, in particolare, il principio di proporzionalità, già al considerando 4 del regolamento si legge che "il diritto alla protezione dei dati di carattere personale non è una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale e va contemperato con altri diritti fondamentali, in ossequio al principio di proporzionalità"[163]. Sul punto occorre fare, però, un'importante precisazione: in questo contesto il principio di proporzionalità assume un valore diverso rispetto a quello assunto nell'articolo 5 TUE, a menzione del quale "La delimitazione delle competenze dell'Unione si fonda sul principio di attribuzione. L'esercizio delle competenze dell'Unione si fonda sui principi di sussidiarietà e proporzionalità". Infatti, mentre nel primo caso serve ad orientare l'agire delle istituzioni europee tutte le volte in cui è necessario bilanciare diversi interessi contrapposti - e assume, pertanto, un valore analogo a quello previsto dal sistema CEDU - nel secondo caso, invece, viene in rilievo per limitare la possibilità di intervento

[162]Vedi articolo 13 direttiva 95/46/CE.

[163]Un riferimento al principio di proporzionalità è contenuto anche nel considerando 22, regolamento (UE) 2016/679 "[omissis] Quando il trattamento dei dati personali effettuato da organismi privati rientra nell'ambito di applicazione del presente regolamento, è opportuno che lo stesso preveda la facoltà per gli Stati membri, a determinate condizioni, di adottare disposizioni legislative intese a limitare determinati obblighi e diritti, qualora tale limitazione costituisca una misura necessaria e proporzionata in una società democratica per la salvaguardia di importanti interessi specifici, comprese la sicurezza pubblica e le attività di prevenzione, indagine, accertamento e perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro, e la prevenzione di, minacce alla sicurezza pubblica. Ciò riveste particolare importanza ad esempio nel quadro del riciclaggio o di attività di medicina legale".

dell'Unione europea nelle materie in cui essa ha competenza concorrente.

2.1.2.2 La direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati

Prima di procedere all'analisi della nuova direttiva (UE) 2016/680, si rende opportuno fare alcune brevi premesse in merito ai cambiamenti apportati dal Trattato di Lisbona alla suddetta disciplina. Invero, prima del 2009 la legislazione in materia di protezione dei dati personali nello spazio di libertà, sicurezza e giustizia era divisa tra il primo pilastro, relativa alla protezione dei dati per fini privati e commerciali e soggetta al metodo comunitario, e il terzo pilastro, relativa, invece, alla protezione dei dati per scopi di ordine pubblico e soggetta al metodo intergovernativo. Com'è noto, la struttura a pilastri è venuta meno con il Trattato di Lisbona e l'articolo 16 TFUE ha attribuito al Parlamento europeo e al Consiglio il potere di legiferare, tramite procedura legislativa ordinaria "con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

Il 4 maggio 2016 è stato pubblicata sulla Gazzetta ufficiale dell'Unione europea, insieme al regolamento (UE) 2016/679, anche la direttiva (UE) 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati", la quale ha abrogato la precedente decisione quadro 2008/977/GAI del Consiglio.

In realtà, facilitare lo scambio e l'accesso di informazioni nello spazio di libertà, sicurezza e giustizia dell'Unione europea rientrava già da anni tra gli obiettivi primari dell'agenda politica europea, poiché ritenuto di fondamentale importanza al fine di contrastare il terrorismo internazionale e aumentare la sicurezza interna[164]. Il miglioramento dello

[164]La Commissione europea nella sua comunicazione del 10 giugno 2009 sull'area di libertà, sicurezza e giustizia a servizio del cittadino rilevava che "security in the EU depends on the effective mechanisms for

scambio di informazioni era infatti uno degli elementi centrali del "Programma dell'Aia", il piano quinquennale dell'Unione europea (2005-2010) per la libertà, giustizia e sicurezza, adottato il 5 novembre del 2004 dal Consiglio europeo in risposta alla "guerra al terrorismo"[165]. Nel successivo "Programma di Stoccolma" (2010-2015), basato su una più stretta cooperazione tra le agenzie dell'Unione europea[166], erano state poi definite alcune politiche che avrebbero dovuto essere adottate ed implementate nella suddetta area.

Passando ora all'analisi del contenuto della direttiva (UE) 2016/680, essa consta di 107 considerando e di 65 articoli. Questi ultimi sono organizzati, a loro volta, in dieci capi. Per quanto riguarda l'oggetto e gli obiettivi della direttiva, all'articolo 1 viene sancito che: "la presente direttiva stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica". La suddetta fonte normativa europea si pone infatti lo specifico obiettivo di contribuire alla realizzazione di uno spazio comune di libertà, sicurezza e giustizia, nel rispetto del diritto fondamentale alla protezione dei dati personali.

In base a quanto evidenziato dal considerando n. 3, l'adozione di una nuova direttiva è divenuta necessaria, dal momento che "[…] la tecnologia, come mai in precedenza, consente il trattamento dei dati personali, come mai in precedenza, nello svolgimento di attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali". Al considerando n. 35 viene inoltre sancito il principio di *necessità*, secondo cui: "per essere lecito, il trattamento dei dati personali a norma della presente direttiva dovrebbe essere necessario per l'esecuzione di un compito svolto nell'interesse pubblico da un'autorità competente in base al diritto dell'Unione o dello Stato membro ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica […]".

---

exchanging information between national authorities and other European players. To achieve this, the EU must develop a «European Information model» based on a more powerful strategic analysis capacity and better gathering and processing of operational information". COM2009 (262), final, pag. 16. Le informazioni in quest'area sono scambiate "to analyse security threats, identify trends in criminal activity or assess risks in related policy areas" COM (2010), 385 final, pag. 26.

[165]Cfr. M. TZANOU, *op. cit.*, v. sopra nota 6, pag. 411. Cfr. anche F. BOEHM, *op. cit.,* v. sopra nota 17, pagg. 1 e ss.

[166]Europol, Eurojust, il sistema di Informazione Schengen (SIS) e il Custom Information System (CIS).

Diversamente da quanto previsto nel regolamento, la direttiva (UE) 2016/680 prevede nell'articolo 6 una diversificazione del trattamento in base alla categoria cui appartiene il soggetto interessato. In particolare, occorre distinguere a seconda che il trattamento riguardi le persone indagate o condannate per un certo reato, oppure le vittime di un reato. La terza categoria è rappresentata, invece, dalle altre parti rispetto a un reato, ovverosia i possibili testimoni o le persone informate sui fatti oggetto delle indagini preliminari e dei procedimenti penali.

Inoltre, al pari del regolamento (UE) 2016/679, anche la direttiva (UE) 2016/680 prevede il cosiddetto *Data Breach*. In particolare, in base a quanto stabilito dall'articolo 30, il titolare del trattamento ha l'obbligo di notificare la violazione dei dati personali all'autorità di controllo al più entro 72 ore da quando ne è venuto a conoscenza, a meno che egli non sia in grado di dimostrare che è la violazione non determini un rischio per i diritti e le libertà delle persone fisiche. È parimenti prevista la possibilità di derogare al limite temporale delle 72 ore qualora il titolare del trattamento dimostri che il ritardo è sorretto da giustificati motivi. L'indicazione del contenuto minimo della notifica è identica a quella prevista dall'articolo 33 del regolamento (UE) 2016/679, il quale ha costituito oggetto di analisi nel paragrafo precedente e a cui si fa integralmente rinvio. Identica è anche la previsione dell'obbligo di notifica direttamente alle persone fisiche, nel caso in cui la violazione dei dati comporti un rischio elevato per i loro diritti e le loro libertà[167]. Infine, il considerando 14 specifica che la direttiva non si applica ai dati raccolti e trattati per ragioni di sicurezza nazionale.

Rispetto alla precedente decisione quadro 2008/977/GAI, la direttiva (UE) 2016/680 ha rinforzato i diritti dell'interessato e imposto nuovi obblighi in capo al titolare e al responsabile del trattamento. Per quanto riguarda, in particolare, i diritti dell'interessato, un'importante novità è rappresentata dal diritto di accesso ai sensi dell'articolo 14. In base alla summenzionata norma, infatti, egli può richiedere al titolare del trattamento conferma che sia o meno in corso il trattamento dei dati personali e, in caso di esito positivo, ottenere l'accesso a diverse informazioni, tra cui quelle relative alle finalità del trattamento, alle categorie dei dati trattati e al loro periodo di conservazione, al diritto di poter richiedere al titolare del trattamento la rettifica, la cancellazione o la limitazione del trattamento dei dati personali che lo riguardano e, inoltre, il diritto di proporre reclamo all'autorità di controllo.

[167]Articolo 31 direttiva (UE) 2016/680.

Un'altra importante novità è rappresentata da un più esteso ambito di applicazione della fonte normativa in esame, che ricomprende anche la prevenzione di minacce alla sicurezza pubblica[168].

Purtuttavia, trattandosi di una direttiva, resta ampio il margine di discrezionalità lasciato agli Stati nel decidere le modalità e gli strumenti tramite cui recepire negli ordinamenti interni il nuovo strumento normativo, considerato, inoltre, che i sistemi penali dei Paesi membri non sono armonizzati. Conseguentemente, il suo ambito di applicazione varierà a seconda della diversa classificazione e definizione fornita dalle leggi nazionali ai diversi tipi di reati, così come alle competenze attribuite alle autorità pubbliche preposte ad investigarli e perseguirli[169]. Al fine di cercare di armonizzare nel miglior modo possibile l'utilizzo della direttiva (UE) 2016/680, l'*Article 29 Working Party* 29 ha recentemente pubblicato un documento "Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)"[170] rivolto principalmente alle DPA (Data Protection Authority), in cui sono stati messi in evidenza gli aspetti più critici della nuova fonte europea e fornite alcune linee guida su come interpretare gli articoli di maggiore rilevanza. In particolare, vengono imposti dei limiti al margine di discrezionalità in capo alle DPA e alle autorità statali al fine di tutelare i diritti degli individui.

Ci si domanda inoltre se, ed in quale misura, la direttiva (UE) 2016/680 possa trovare applicazione anche nell'ambito della raccolta e del trattamento dei dati personali da parte delle agenzie europee che operano nello spazio di libertà, sicurezza e giustizia. Invero, lo scambio di informazioni personali, principalmente fra le agenzie Europol, Eurojust, Frontex e OLAF, è divenuto negli ultimi anni uno strumento fondamentale per garantire la sicurezza interna dell'Unione europea[171]. Si consideri, inoltre, che le varie autorità giudiziarie e di polizia degli Stati membri attingono in maniera sempre più consistente per le loro attività dai diversi *data base* appartenenti ai cosiddetti Sistemi europei di Informazione, di cui fanno parte il sistema di comunicazione e informazione

[168]Cfr. P.-Y MONJAL, *op. cit.*, v. sopra nota 155, pag. 635.
[169]Cfr. T. QUINTEL, *Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive*, in *European Data Protection Law Review* 2018, pag. 104.
[170]Article 29 Working Party (WP29), *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680),* 29 Novembre 2017, 17/EN, WP 258.
[171]Cfr. F. BOEHM, *Information Sharing in the Area of Freedom, Security and Justice – Towards a Common Standard for Data Exchange Between Agencies and EU Information System,* in S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET, *European Data Protection: In Good Health?,* Springer 2012, pag. 143.

(CIS), il sistema di Informazione Schengen (SIS), il Sistema di Informazione Visti (VIS) e, infine, l'EURODAC. La necessità di una maggiore interoperabilità fra i diversi sistemi di raccolta dati personali delle agenzie europee era stato d'altronde già auspicato nel precedentemente citato programma di Stoccolma adottato dal Consiglio europeo nel 2010[172]. L'interoperabilità rappresentava infatti, nella visione degli autori del programma, "a precondition for the efficency of police and judicial cooperation in the AFSJ"[173]. Ciononostante, la direttiva (UE) 2016/680 si limita a disciplinare la raccolta e il trattamento dei dati personali da parte degli Stati membri, escludendo, invece, dal proprio ambito di applicazione quelli effettuati da istituzioni o agenzie dell'Unione europea[174]. Analoga disposizione è prevista anche dall'articolo 2, par. 3, del regolamento (UE) 2016/679. Conseguentemente, nei confronti dei dati trattati da Europol, Eurojust, Frontex e OLAF, o dai diversi Sistemi europei di Informazione, continuerà a trovare applicazione il regolamento (UE) 2001/45 "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", con l'auspicio di provvedere ad adattare i principi in esso contenuto alla nuova normativa europea. La mancata estensione dell'ambito di applicazione del "Pacchetto protezione dati" anche ai dati trattati dalle agenzie europee che operano nel settore dello spazio di libertà, sicurezza e giustizia, ha fatto sì che la disciplina in materia continui ad essere ad oggi non armonizzata, con conseguenze negative anche per i diritti dei singoli, che avrebbero potuto beneficiare, invece, anche in questo contesto delle maggiori tutele offerte dal regolamento (UE) 2016/679 e dalla direttiva (UE) 2016/680[175].

[172]Consiglio europeo, *Programma di Stoccolma*, *Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, 4 maggio 2010, 2010/C 115/01, par. 4.2.
[173]F. BOEHM*, op. cit.*, v. sopra nota 171, pag. 173.
[174]Art. 2, par. 3, direttiva (UE) 2016/680.
[175]F. BOEHM, *Data processing and law enforcement access to information systems at EU level*, *No consistent framework in spite of the envisaged data protection reform*, in *Datenschutz and Datensicherheit* tion 2012, pag. 343.

2.1.2.2.1 Le clausole di limitazione nella direttiva (UE) 2016/680

Diversamente da quanto previsto nel regolamento, ove la clausola di limitazione è contenuta espressamente nell'articolo 23, nella direttiva (UE) 2016/680 manca una corrispondente disposizione a riguardo. Ciononostante, la possibilità per gli Stati di derogare in particolari circostanze è ricavabile da diversi articoli del testo legislativo, ove vengono previste delle limitazioni con riferimento, rispettivamente, al diritto di informazione e di accesso ai dati riconosciuti in capo all'interessato. L'articolo 13, paragrafo 3, e l'articolo 15 prevedono infatti che gli Stati possano adottare misure volte a ritardare, limitare o escludere la comunicazione e l'accesso alle informazioni relative al trattamento dei dati, nei limiti e nella misura in cui queste siano *necessarie* e *proporzionate* in una società democratica, al fine di non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, proteggere la sicurezza pubblica, proteggere la sicurezza nazionale, proteggere i diritti e le libertà altrui. Qualora lo Stato decida di usufruire della clausola di limitazione prevista dagli appena esaminati articoli, il titolare del trattamento ha l'obbligo di informare senza ritardo l'interessato, indicando i motivi del rifiuto o della limitazione. La suddetta comunicazione può essere omessa nel caso in cui ne possa derivare un rischio per le indagini.

È inoltre prevista la possibilità di omettere o ritardare la notifica del Data Breach per "[…] non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari, per non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, proteggere la sicurezza pubblica o la sicurezza nazionale o tutelare i diritti e le libertà altrui"[176].

In ogni caso, le limitazioni devono sempre avvenire nel rispetto dei diritti fondamentali sanciti dalla Carta, dal TFUE "[…] in particolare (del) diritto al rispetto della vita privata e familiare, il diritto alla protezione dei dati personali e il diritto a un ricorso effettivo e a un giudice imparziale. Conformemente all'articolo 52, paragrafo 1, della Carta, eventuali limitazioni di tali diritti possono essere apportate solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui"[177].

[176]Considerando 44 direttiva (UE) 2016/680.
[177]*Ibidem*, considerando 107.

Un ulteriore elemento a favore di una tutela più effettiva ed uniforme per i diritti dei singoli è rappresentato dalla possibilità - fortemente auspicata - per gli Stati membri di prevedere che le funzioni di vigilare il rispetto del regolamento (UE) 2016/679 e della direttiva (UE) 2016/680 siano svolte da un'unica autorità di controllo[178]. Un'unica autorità di controllo garantirebbe, infatti, un'interpretazione più omogenea dei principi comuni alla due fonti normative europee e una maggiore coerenza nell'applicazione delle stesse.

2.1.2.3 La direttiva (UE) 2016/681 sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e azione penale nei confronti dei reati di terrorismo e reati gravi

Come già precedentemente analizzato, tra le principali minacce al rispetto del diritto fondamentale alla protezione dei dati personali si rinvengono anche il loro uso e la loro trasmissione a Paesi terzi - in particolare agli Stati Uniti - ove gli standard di tutela possono risultare inferiori. Si pensi, ad esempio, alla trasmissione dei codici passeggeri di volo PNR e a quelli bancari TFTP.

Al fine di arginare i suddetti rischi, il 27 aprile 2016 l'Unione europea ha adottato, nell'ambito del precitato Programma di Stoccolma[179] relativo allo spazio di libertà, sicurezza e giustizia, la direttiva (UE) 2016/681 che disciplina l'utilizzo dei codici di prenotazione, o PNR, dei passeggeri dei voli internazionali da parte degli Stati membri[180]. La suddetta direttiva fa parte delle misure adottate nell'ambito della cosiddetta Unione Sicurezza, creata in seguito ai diversi attacchi terroristici che hanno interessato l'Europa a partire dal 2015[181]. Con tale termine la Commissione indica, in particolare, l'insieme di tutte le misure legislative volute e messe in atto al fine di proteggere in maniera più efficace i cittadini europei e creare uno spazio comune più sicuro.

In base a quanto previsto dall'articolo 3 della direttiva (UE) 2016/681, i dati PNR vengono definiti come l'insieme di tutte "le informazioni relative al viaggio di ciascun

[178]Articolo 41, par. 3, direttiva (UE) 2016/680.
[179]Vedi paragrafo 2.1.2.2.
[180]Cfr. F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR*? In *Diritti umani e diritto internazionale*, 2017, pag. 213 e ss.
[181]*Communication from the Commission to European parliament, the European Council and the Council on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union*, Bruxelles, 20 aprile 2016 COM(2016) 230 final, disponibile alla pagina https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf.

passeggero comprendenti i dati necessari per il trattamento e il controllo delle prenotazioni a cura dei vettori aerei e di prenotazione interessati per ogni volo prenotato da qualunque persona o per suo conto, siano esse registrate in sistemi di prenotazione, in sistemi di controllo delle partenze utilizzato per la registrazione dei passeggeri sui voli, o in altri sistemi equivalenti con le stesse funzionalità".

L'utilizzo dei dati PNR, così come sottolineato dal considerando n. 7, rappresenta uno strumento efficace per contrastare la minaccia del terrorismo internazionale e di altri gravi reati "[...] Tuttavia, affinché il trattamento dei dati PNR rimanga nei limiti di ciò che è necessario, è opportuno che la definizione e l'applicazione dei criteri di valutazione siano limitate ai reati di terrorismo e a reati gravi per cui l'uso di tali criteri risulta pertinente. Inoltre, i criteri di valutazione dovrebbero essere definiti in maniera da ridurre al minimo il numero di persone innocenti erroneamente identificate dal sistema"[182].

In ogni caso, lo scambio di dati PNR deve essere realizzato nel rispetto del diritto alla vita privata e familiare garantito sia dalla Carta dei diritti fondamentali dell'Unione europea, sia dalla Convenzione 108 del 1981, sia, infine, dalla CEDU[183].

L'articolo 1 definisce l'ambito di applicazione della direttiva (UE) 2016/681, che concerne il trasferimento a cura dei vettori aerei dei dati del codice di prenotazione dei passeggeri (PNR) dei voli extra-UE (a) e il trattamento dei dati di cui alla lettera a), comprese le operazioni di raccolta, uso e conservazione a cura degli Stati membri e il loro scambio tra gli Stati membri. Il paragrafo 2 specifica, poi, che i suddetti dati devono essere trattati al solo fine di contrastare il terrorismo internazionale o prevenire la commissione di gravi reati".

Ai sensi dell'articolo 2, gli Stati membri possono applicare la direttiva (UE) 2016/682 anche con riferimento ai voli intra-europei, purché questo venga notificato alla Commissione europea.

La direttiva (UE) 2016/681 impone inoltre agli Stati membri di creare una propria "Unità di informazione sui passeggeri" (UIP), con il compito di raccogliere e scambiare i dati PNR dalle compagnie aeree[184]. I dati possono essere conservati per un periodo non superiore ai cinque anni[185] ma, dopo sei mesi dal trasferimento degli stessi all'UIP dello

[182]Considerando 7 direttiva (UE) 2016/680.
[183]Considerando 23 direttiva (UE) 2016/680.
[184]Articolo 4 direttiva (UE) 2016/680.
[185]Articolo 12 direttiva (UE) 20160/680.

Stato membro dal cui parte o atterra il volo, esso vengono anonimizzati mediante la mascheratura di alcuni elementi, quali il nome, l'indirizzo, le modalità di pagamento, che potrebbero portare all'identificazione diretta del passeggero.
Infine, gli Stati membri possono anche decidere di raccogliere e trattare i dati PNR provenienti da operatori economici diversi dalle compagnie aeree, come le agenzie di viaggio e gli operatori turistici, che forniscono servizi di prenotazione di voli e, quindi, raccolgono e trattano dati PNR.

2.1.2.4 La proposta di regolamento *e-privacy*

Nel febbraio del 2017 la Commissione europea ha presentato la proposta del nuovo regolamento in materia di comunicazioni elettroniche[186], il quale, una volta approvato, sostituirà la direttiva 2002/58/CE, dichiara invalida con la sentenza *Tele2 Sverige AB.*[187]. Nonostante la sua invalidità, la suddetta direttiva ha avuto il merito di introdurre per la prima volta il concetto di "l'Internet" nel sistema normativo europeo[188].
In ragione del crescente sviluppo tecnologico e dell'uso sempre più massiccio dei mezzi di comunicazione e dei *social media*, si è resa necessaria una nuova proposta legislativa, la quale assumerà le forme del regolamento e sarà quindi direttamente vincolante per gli Stati membri. Se da un lato infatti, i nuovi strumenti tecnologici hanno facilitato le comunicazioni e l'accesso alle informazioni, dall'altro lato a fronte delle nuove opportunità si presentano anche nuovi pericoli rappresentati, per esempio, dallo *spyware,* dai *web bugs* e, infine, dai *cookies*.
Il nuovo regolamento, che consta di 43 considerando e 29 articoli, è divenuto necessario al fine di rendere operativo l'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. La base giuridica del suddetto regolamento è rappresentata dagli articoli 16 e 114 TFUE e si ispira ai principi di sussidiarietà, proporzionalità (inclusione OTT, meccanismo di coerenza, margini di deroga agli Stati membri per fini legittimi), dimensione

[186]Proposta di regolamento del Parlamento europeo e del Consiglio *relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE* (regolamento sulla vita privata e le comunicazioni elettroniche), Bruxelles, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).
[187]Corte di giustizia (Grande Sezione), *Tele2 Sverige AB*, cit..
[188]Considerando n. 6 direttiva 2002/58/CE "L'Internet ha sconvolto le tradizionali strutture del mercato fornendo un'infrastruttura mondiale comune per la fornitura di un'ampia serie di servizi di comunicazione elettronica. I servizi di comunicazione elettronica accessibili al pubblico attraverso l'Internet aprono nuove possibilità agli utenti ma rappresentano anche nuovi pericoli per i loro dati personali e la loro vita privata".

transfrontaliera delle problematiche in ragione della tecnologia Internet e digitale, obiettivo mercato digitale e, infine, logica partecipazione alla consultazione pubblica.

Con riferimento inoltre al regolamento (UE) 2016/679, la Commissione europea ha specificato che tra le due fonti normative intercorre un rapporto di genere/specie, in cui il regolamento sulle comunicazioni elettroniche costituisce una specificazione della disciplina dettata dal regolamento (UE) 2016/679. Le due fonti normative si differenziano, inoltre, per l'oggetto: il primo si occupa della tutela dei dati personali, mentre il secondo della confidenzialità delle comunicazioni.

2.1.2.4.1 La clausola di limitazione nella proposta di regolamento *e-privacy*

Anche la nuova proposta di regolamento prevede, in linea con le altre disposizioni normative precedentemente analizzate in materia di protezione dei dati personali, la possibilità per gli Stati di limitare la tutela dei diritti invocando la clausola di deroga. In particolare, l'articolo 11 prevede che l'Unione europea o gli Stati membri possano adottare delle misure limitative alla tutela dei dati personali a condizione che queste rispettino "[…] the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679 or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests […]"[189].

La norma in esame richiama, tra gli "interessi generali" che giustificano la deroga, quelli elencati nell'articolo 23 del regolamento (UE) 2016/679 – che sono d'altronde gli stessi indicati anche nella direttiva (UE) 2016/680 – per l'analisi dei quali si rinvia a quanto già precedentemente esposto nel paragrafo 2.1.2.1.1.

[189]Articolo 11, Proposta di regolamento del Parlamento europeo e del Consiglio *relativo al rispetto della vita privata e alla tutela dei dati personali nelle comunicazioni elettroniche e che abroga la direttiva 2002/58/CE* (regolamento sulla vita privata e le comunicazioni elettroniche), Bruxelles, 10.1.2017 COM(2017) 10 final 2017/0003 (COD).

2.2 LA TUTELA DEI DATI PERSONALI NEL SISTEMA REGIONALE DEL CONSIGLIO D'EUROPA

2.2.1 L'articolo 8 CEDU

Per quanto riguarda invece il sistema previsto dal Consiglio d'Europa, la concezione del diritto alla protezione dei dati personali, così come la intendiamo oggi, costituisce il frutto di un lungo e progressivo percorso di elaborazione giurisprudenziale, iniziato negli anni '80 con il noto caso *Klass e altri c. Germania*[190] e, per alcuni versi, ad oggi non ancora terminato. La CEDU non prevede infatti alcun norma che tuteli nello specifico i dati personali "di qui la necessità di un attento e approfondito esame delle sentenze della Corte europea dei diritti dell'uomo e delle decisioni della Commissione per valutare come attraverso esse si sia definito il concetto di «vita privata», in che modo e in quali circostanze ne sia stata constatata la violazione e come siano state interpretate le eccezioni previste nel secondo comma dell'art. 8"[191]. Si può ormai ritenere pacifico che i dati personali rientrino a pieno regime nell'alveo dell'articolo 8 CEDU[192].

Si rileva inoltre che, nonostante la giurisprudenza relativa all'interpretazione ed applicazione dell'8 CEDU sia molto ampia – superando di gran lunga il migliaio di pronunce[193] - ad oggi siano pochissimi i casi portati di fronte alla Corte europea dei diritti umani relativi alle intercettazioni telefoniche, alla tutela dei dati personali su Internet e, in generale, a tutte le problematiche connesse alle nuove tecnologie e al bisogno di far fronte alle nuove minacce terroristiche. Con riferimento a quest'ultimo aspetto, si può infatti affermare le misure limitative ai diritti siano giustificate principalmente alla luce dell'articolo 2 della stessa Convenzione, che sancisce l'obbligo in capo agli Stati membri di adottare misure legislative volte a proteggere la vita umana. Invero, come si ha già avuto modo di evidenziare nel precedente capitolo, i diritti umani si distinguono in diritti relativi, tra cui si annoverano il diritto alla privacy e alla libertà di espressione che possono subire limitazioni a determinate condizioni, e diritti assoluti, come il divieto di tortura e

[190]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania,* 6 settembre 1978, ricorso n. 5029/1971.
[191]Cfr. A. BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Rivista Internazionale dei diritti dell'Uomo* 1999, pag. 543.
[192]Cfr. M. NINO, *Terrorismo Internazionale, privacy e protezione dei dati personali*, Editoriale Scientifica, Napoli 2012, pag. 70.
[193]Cfr. F. PAEFGEN, *Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet*, Springer, Heidelberg 2017, pag. 3.

trattamenti inumani e degradanti previsto all'articolo 3 CEDU[194], che non possono subire limitazioni di alcuna sorta.

L'articolo 8, comma 1, CEDU stabilisce che "Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza". Già ad un'analisi letterale del dettato normativo si può ricavare la prima suddivisione del diritto alla privacy in tre diverse sottocategorie, ossia appunto la vita privata e familiare, il domicilio e, infine, la corrispondenza. Nel corso degli anni, poi, sono stati fatti rientrare nell'alveo dell'articolo 8 CEDU anche altri aspetti connessi alla vita dell'individuo, relativi soprattutto alle interazioni dello stesso con il mondo esterno e con le altre persone. Tra questi vi rientrano l'integrità fisica e morale[195], l'identità sessuale[196], il diritto al nome[197], la protezione dell'ambiente[198], il trattamento dei dati sanitari e DNA[199] e, infine la tutela dell'onore e della reputazione che, si ricordi, a differenza dell'articolo 17 del Patto sui diritti civili e politici analizzato nel primo capitolo[200], non è espressamente sancita a livello normativo ma costituisce il frutto di un'evoluzione giurisprudenziale.

Per quanto riguarda l'ambito applicativo della norma in esame, dopo un iniziale orientamento secondo cui l'articolo 8 CEDU avrebbe riguardato solamente la tutela dell'individuo nei confronti delle autorità pubbliche, se n'è andato consolidandosi un altro

---

[194]Consiglio d'Europa, *Les droits de l'homme et la lutte contre le terrorisme: les lignes directrices du Conseil de l'Europe,* Strasburgo 2002, pag. 8.

[195]Corte europea dei diritti umani, *X e Y c. Paesi Bassi*, sentenza del 26 marzo 1985, ricorso n. 8978/80; Corte europea dei diritti umani, *Bensaid c. Regno Unito*, sentenza del 6 febbraio 2001, ricorso n. 44599/98.

[196]Corte europea dei diritti umani, *Y.Y. c. Turchia*, sentenza del 10 marzo 2015, ricorso n. 14793/08; Corte europea dei diritti umani, *Schalk e Kopf c. Austria*, sentenza del 24 giugno 2010, ricorso n. 30141/04; Corte europea dei diritti umani, *Mosley c. Regno Unito*, sentenza del 10 maggio 2011, ricorso n. 48009/08; Corte europea dei diritti umani, *Schlumpf c. Svizzera*, sentenza dell'8 gennaio 2009, ricorso n. 29002/06; Corte europea dei diritti umani, *L. c. Lituania*, sentenza dell'11 settembre 2007, ricorso n. 27527/03; Corte europea dei diritti umani, *Christine Goodwin c. Regno Unito*, sentenza dell'11 luglio 2002, ricorso n. 28957/95.

[197]Corte europea dei diritti umani, *Muna Macalin Moxamed Sed Dahir c. Svizzera*, sentenza del 15 settmbre 2015, ricorso n. 12209/10; Corte europea dei diritti umani, *Cusan e Fazzo c. Italia*, sentenza del 7 gennaio 2014, ricorso n. 77/07; Corte europea dei diritti umani, *Losonci Rose e Rose c. Svizzera*, sentenza del 9 novembre 2010, ricorso n. 664/06; Corte europea dei diritti umani, *Kemal Taskin e altri c. Turchia*, 2 febbraio 2010, ricorsi nn. 30206/04; Corte europea dei diritti umani, *Daroczy c. Ungheria*, sentenza del 1 luglio 2008, ricorso n. 44378/05.

[198]Corte europea dei diritti umani, *Di Sarno e altri c. Italia,* sentenza del 10 gennaio 2012, ricorso n. 30765/08.

[199]Corte europea dei diritti umani (GC), *S. e Marper c. Regno Unito*, sentenza del 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04; Corte europea dei diritti umani, *L.H. c. Lettonia*, sentenza del 29 aprile 2014, ricorso n. 52019/07.

[200]Articolo 17 Patto sui diritti civili e politici "Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e alla sua reputazione. Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".

più estensivo, tuttora in vigore, in base al quale la norma "[…] s'impose aux particuliers comme aux autorités publiques"[201].

Orbene, tornando alle *sub*-categorie iniziali, pare necessario soffermarsi in particolare sulla tutela della corrispondenza, data anche l'evoluzione che il concetto ha subito in ragione del recente sviluppo tecnologico e, come si avrà modo di vedere grazie all'analisi dei recenti casi decisi dalla Corte europea dei diritti umani, delle limitazioni operate per ragioni di sicurezza nazionale e *law enforcement*. Invero, il concetto di corrispondenza è molto ampio e sembra essere arrivato a ricomprendere oggi tutte le informazioni scambiate sul *web* dagli individui, quali possono essere ad esempio le email, i messaggi di testo tramite applicazioni come *Whatsapp* e *Skype* o tutti gli altri mezzi di comunicazione creati negli ultimi anni grazie al progresso digitale[202].

Per ragioni di completezza si ritiene opportuno menzionare, pur non potendo in questa sede analizzare la questione nel dettaglio per ragioni connesse all'oggetto di indagine, un'altra problematica, più di natura sociologica, emersa negli ultimi anni con riferimento a questi nuovi mezzi di comunicazione. Infatti, se da un lato è pacifico che le comunicazioni scambiate tramite i prima menzionati strumenti tecnologici siano di natura privata, e pertanto tutelabili ai sensi dell'articolo 8 CEDU, dall'altro lato numerosi dubbi vengono nutriti, invece, in relazione a tutte le informazioni condivise quotidianamente, e pertanto pubblicamente accessibili, dagli utenti sulle piattaforme online, quali possono essere, ad esempio, i blog e i *social network*. Il crescente bisogno di condivisione ha di fatto aumentato in maniera esponenziale la quantità di dati personali messi a disposizione, in maniera più o meno consapevole, dagli individui nel cyberspazio. Le suddette informazioni, una volta pubblicate, possono circolare liberamente e venire raccolte ed immagazzinate non solo dalle autorità pubbliche, che possono utilizzarle per ragioni connesse al potenziamento delle attività di *law enforcement* e alla necessità di tutelare la sicurezza nazionale, ma anche dai soggetti privati, la cui unica finalità è quella di trarne profitto.

Invero questo fenomeno, pur apportando diversi vantaggi in termini di sicurezza collettiva - con riferimento soprattutto alla cosiddetta *social media intelligence*, ossia al potenziale utilizzo dei dati personali condivisi sui social network per prevenire gli attacchi terroristici

[201]M.J. VELU, *La Convention européenne des droits de l'homme et le droit au respect de la vie privée, du domicile et des communications*, in *Vie privée et droits de l'homme*, Bruylant-Bruxelles 1973, pag. 48.
[202]Cfr. F. PAEFGEN, *op. cit.*, v. sopra nota 193, pag. 18.

e geolocalizzare i responsabili dei suddetti crimini – cela numerosi rischi per la privacy degli individui, dovuti anche alla mancanza, sia a livello normativo sia a livello giurisprudenziale, di una qualche, seppure basilare, regolamentazione in materia. Accanto al controllo della corrispondenza, un'ulteriore modalità di interferenza con il diritto alla protezione dei dati personali sancito dall'articolo 8 CEDU è rappresentata, nel contesto in esame, dalle intercettazioni telefoniche. Di esse la polizia si avvale principalmente nelle sue indagini investigative, siano esse di natura preventiva – ossia finalizzate all'identificazione di possibili minacce alla sicurezza nazionale – o repressiva, volte cioè a rintracciare gli autori dei crimini già commessi. Molto significativo a riguardo è il caso *Malone c. Regno Unito*[203], in cui la Corte europea dei diritti umani ha riconosciuto che le suddette intercettazioni possono costituire un'ingerenza nel diritto alla privacy.

2.2.1.1 Le limitazioni all'articolo 8 CEDU

In materia di tutela della privacy, è lo stesso articolo 8 CEDU, secondo comma, a prevedere i limiti e le modalità con cui le limitazioni possono avere luogo. Ivi viene infatti stabilito che la misura di interferenza è legittima solo se "[…] 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".

La norma in esame ha costituito oggetto di numerose sentenze della Corte europea dei diritti umani, ove sono state specificati e descritti in maniera analitica i requisiti necessari per limitare in maniera legittima l'articolo 8 CEDU. La misura di restrizione deve, infatti, essere prevista dalla legge, perseguire uno scopo legittimo ed essere necessaria in una società democratica. Un'analoga disposizione è prevista, inoltre, dall'articolo 52, par. 1, della Carta dei diritti fondamentali dell'Unione europea, secondo cui "1. Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate

[203]Corte europea dei diritti umani (Plenaria), *Malone c. Regno Unito*, sentenza del 2 agosto 1984, ricorso n. 8691/1979.

limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".

Per quanto riguarda, innanzitutto, il requisito "previsto dalla legge" – utilizzando l'espressione francese "prévue par la loi" e venendo la legge generalmente intesa nella sua accezione sostanziale, ossia ricomprendente il diritto scritto e non scritto, e non solo in quella formale[204] - la Corte ha affermato che, in primo luogo, la misura di interferenza deve avere una base nella legge nazionale[205] e deve essere rispettosa dello Stato di diritto. In secondo luogo, poi, la legge deve essere adeguatamente accessibile "[…] the citizen must be able to have an indication that is adequate, in the circumstances, of the legal rule applicable to a given case"[206]. Infine, la legge deve essere formulata con sufficiente precisione, per consentire all'individuo di orientare la propria condotta e conformarsi ad essa[207]. Qualora si renda, inoltre, necessario adottare delle misure che, al fine di tutelare ad esempio la sicurezza nazionale, possano in qualche modo limitare le libertà e i diritti fondamentali degli individui, il legislatore deve predisporre tutte le garanzie idonee per contrastare eventuali abusi, posti in essere soprattutto dal potere esecutivo. Invero, una legge che conferisce discrezionalità deve essere sufficientemente prevedibile – la Corte utilizza l'aggettivo "*foreseebility*" – e indicare con chiarezza lo scopo delle misure limitative del diritto, nonché i mezzi a disposizione del singolo per fare valere le proprie pretese in sede giurisdizionale[208]. Nel contesto delle misure di sorveglianza di massa, il principio della prevedibilità assume una primaria importanza al fine di delimitare il potere discrezionale degli Stati[209], così com'è stato d'altronde recentemente ribadito dalla Corte

[204]Cfr. P. MAHONEY, F. MATCHER, H. PETZOLD, L. WILDHABER, *Protection des droits de l'homme: la perspective européenne*, Carl Heymanns Verlag KG-Koeln-Berlin-Bonn-Muenchen, Colonia 2000, pag. 382. Questo principio è stato inoltre affermato a livello giurisprudenziale nel caso della Corte europea dei diritti umani (Plenaria), *Sunday Times c. Regno Unito,* sentenza del 26 aprile 1979, ricorso n. 6538/74, par. 47.

[205]Cfr. Corte europea dei diritti umani, *Silver e altri c. Regno Unito*, sentenza del 25 marzo 1983, ricorsi nn. 5947/72 e altri, par. 85; (Plenaria) *Malone c. Regno Unito,* sentenza del 2 agosto 1984, ricorso n. 8691/1979, par. 66.

[206]Corte europea dei diritti umani (Plenaria), *Sunday Times c. Regno Unito*, cit., par. 49.

[207]Corte europea dei diritti umani, *von Hannover c. Germania,* sentenza del 24 giugno 2004, ricorso n. 59320/00, parr. 74-75 e 77; Corte europea dei diritti umani (GC), *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, sentenza del 27 giugno 2017, ricorso n. 931/13, parr. 143-148; Corte europea dei diritti umani (GC) *Delfi As c. Estonia*, ricorso n. 64569/09, sentenza del 10 ottobre 2013, par. 121. Cfr. in dottrina Y. ARAI-TAKANASHI, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*, Antwerpen-Oxford-New York, Intersentia 2002, pag. 61.

[208]Corte europea dei diritti umani, *Olsson v. Svezia*, 24 marzo 1988, ricorso n. 10465/83.

[209]La Corte di Stasburgo parla di "foreseeability" già a partire dalle prime pronunce in tema di misure di sorveglianza e limitazioni al diritto alla privacy. Vedi, ad esempio, Corte europea dei diritti umani, *Malone c.*

europea dei diritti umani nel caso *Roman Zakharov c. Russia*: "[…] foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly. However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident. It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated [...]"[210].

Il secondo requisito richiesto dall'articolo 8, comma 2 CEDU, ossia che la misura limitativa debba perseguire uno scopo legittimo, non ha costituito fonte di particolari dibattiti in seno agli Stati membri del Consiglio d'Europa, dal momento che l'adesione alla CEDU presuppone già di per sé un forte impegno da parte degli Stati a promuovere e a fare rispettare i principi democratici e i diritti umani[211], per cui è implicito che le misure limitative debbano essere adottate nel rispetto dello stato di diritto. Tra gli scopi legittimi maggiormente invocati dagli Stati vi rientrano, ad esempio, la pubblica sicurezza, il benessere economico del paese, la protezione dei diritti e delle libertà fondamentali, il bisogno di prevenire disordini e crimini.

Con riferimento al requisito "necessary in a democratic society", la Corte europea dei diritti umani nella sua giurisprudenza[212] specifica che, innanzitutto, l'aggettivo "necessario" non è sinonimo di "indispensabile", né tantomeno può essere ricondotto ad espressioni più generiche e flessibili quali "utile", "desiderabile". Il requisito "necessaria in una società democratica" sta infatti a significare che la misura, per essere compatibile con la Convenzione, deve corrispondere ad un "pressante bisogno sociale" ed essere "proporzionata rispetto allo scopo legittimo perseguito"[213].

Nel decidere quali misure da adottare sono necessarie, gli Stati contraenti godono in di un certo margine di discrezionalità, soggetto sempre al rigido scrutinio della Corte, che

---

Regno Unito, cit., par. 67; Corte europea dei diritti umani, *Leander c. Svezia*, sentenza del 26 marzo 1987, ricorso n. 9248/81, par. 51.

[210]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., par. 229; cfr. anche Corte europea dei diritti umani, *Shimovolos c. Russia,* sentenza del 21 giugno 2011, ricorso n. 30194/09, par. 68.

[211]Cfr. Y. ARAI-TAKANASHI, *op. cit.*, v. sopra nota 207, pag. 62.

[212]Corte europea dei diritti umani, *Silver e altri c. Regno Unito*, 24 settembre 1982, ricorsi nn. 5947/72 e altri, par.97.

[213]Corte europea dei diritti umani, *Leander c.Svezia*, cit., par. 58.

ha sempre l'ultima parola in merito alla loro compatibilità con l'articolo 8, par. 2 della Convenzione. A tale scopo, le autorità nazionali devono assicurarsi che le misure siano *rilevanti* e *sufficienti* rispetto agli scopi perseguiti dall'articolo 8 CEDU. Il test della rilevanza, che è strettamente connesso al requisito dello scopo legittimo perseguito di cui al paragrafo 2 dell'articolo 8 CEDU, è agevolmente riconoscibile. Per contro, il test della sufficienza necessita di una più approfondita analisi di alcuni fattori quali la natura delle misure, la loro severità, nonché gli eventuali rischi e pericoli per i diritti degli individui. Inoltre, il test della sufficienza è strettamente connesso al giudizio di proporzionalità, dal momento non può essere fatta nessuna valutazione sul rapporto fra i diritti degli individui e gli interessi della società a meno che le misure adottate non siano sufficientemente giustificate[214]. Infine, sempre in base alla giurisprudenza di Strasburgo, i paragrafi della Convenzione che consentono delle limitazioni ai diritti devono essere interpretati restrittivamente.

Come si avrà modo di analizzare in maniera approfondita nel prosieguo della trattazione, l'articolo 8 CEDU, che sancisce il diritto al rispetto alla vita privata e familiare, non contiene un'espressa indicazione sulla tutela dei dati personali. La mancanza di un simile riferimento è facilmente intuibile se si considera il contesto storico-politico in cui la CEDU è stata approvata. Invero, quando nel 1952 la Convenzione di Roma è entrata in vigore non esisteva ancora una nozione di dati personali così come la intendiamo oggi, né era lontanamente prevedibile la diffusione che i suddetti dati avrebbero potuto subire nei successivi decenni[215]. L'inclusione della tutela dei dati personali nell'alveo dell'articolo 8 CEDU è quindi il frutto di un progressivo, e relativamente recente, sviluppo giurisprudenziale.

Occorre, infine, ricordare che, alla pari di quanto interpretato con riferimento all'articolo 17 del Patto sui diritti civili e politici, l'articolo 8 CEDU non contiene solo obblighi negativi ma obblighi di natura positiva a carico dello Stato al fine di garantire appieno il diritto dell'individuo[216]. Questo concetto è stato introdotto per la prima volta dalla Corte

[214]Cfr. Y. A. TAKAHASHI*, op. cit.*, v. sopra nota 208, pag. 63.
[215]F. PAEFGEN, *op. cit.*, v. sopra nota 193, pag. 3.
[216]Cfr. Corte europea dei diritti umani (Plenaria), *Gaskin c. Regno Unito*, sentenza del 7 luglio 1989, ricorso n. 10454/83, par. 40. In dottrina cfr. Y. ARAI-TAKANASHI e altri, *op. cit.,* v. sopra nota 128, pagg. 739-747.

europea dei diritti umani nel caso *Marckx*[217] e poi successivamente ribadito nella pronuncia *X e Y c. Paesi Bassi*[218].

2.2.2 La Convenzione 108 del Consiglio d'Europa

Il 28 gennaio 1981 il Comitato dei Ministri del Consiglio d'Europa ha adottato la *Convenzione 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale*, che ha lo specifico scopo di arginare la divulgazione dei dati personali a soggetti terzi non autorizzati. La Convenzione 108 rappresenta il primo, e ad oggi unico, strumento internazionale di natura vincolante in materia di dati personali. Essa istituisce inoltre una cooperazione fra gli Stati contraenti, grazie al Comitato consultivo previsto dalla Convenzione stessa[219].

Per quanto riguarda il contenuto, l'articolo 1 individua innanzitutto l'oggetto e lo scopo del Trattato, che è quello "[…] di garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque sia la sua cittadinanza o residenza, il rispetto dei diritti e delle libertà fondamentali, ed in particolare del diritto alla vita privata, nei confronti dell'elaborazione automatizzata dei dati di carattere personale che la riguardano («protezione dei dati»)". È molto significativo il fatto che la Convenzione abbia circoscritto la sua portata alla sola tutela dei dati personali. Da questo elemento si ricava infatti che, nella concezione dei fautori del trattato internazionale, la protezione dei dati personali era strettamente connessa, ma non corrispondeva esattamente, al diritto alla privacy. Ciò era estremamente innovativo considerata l'epoca di entrata in vigore della Convenzione.

Passando poi all'analisi delle successive disposizioni, l'articolo 2, lettera a) specifica il significato del termine dati personali: "ogni informazione relativa a una persona fisica identificata o identificabile (persona interessata)"; mentre alla lettera c viene data una definizione di "elaborazione automatizzata": c) "l'elaborazione automatizzata comprende le seguenti operazioni effettuate nel loro insieme o in parte grazie a procedimenti automatizzati: registrazione di dati, applicazione ad essi di operazioni logiche e/o aritmetiche, loro modifica, cancellazione, estrazione o diffusione".

[217]Corte europea dei diritti umani, *Marckx c. Belgio*, sentenza del 13 giugno 1979, ricorso n. 6833/74, par. 31.
[218]Corte europea dei diritti umani, *X e Y c. Paesi Bassi*, cit., par. 23.
[219]Cfr. F. MARTINES, *op. cit*., v. sopra nota 46, pag. 724.

Di particolare importanza è inoltre l'articolo 3, che stabilisce l'ambito di applicazione del Trattato. In particolare, la Convenzione si applica alla raccolta e all'elaborazione automatica dei dati nel settore pubblico e in quello privato.

È in ogni caso prevista la possibilità per gli Stati contraenti di limitare, nel rispetto di specifiche condizioni formali e procedurali, la portata applicativa del Trattato. In particolare, ai sensi dell'articolo 3, lettere a) b) e c), ogni Stato può in qualsiasi momento comunicare al Segretario generale del Consiglio dei Ministri di non applicare la Convenzione a certe categorie automatizzate di dati personali, ovvero di applicarla anche ad informazioni relative a gruppi di persone, associazioni, fondazioni, società, corporazioni, o a qualsiasi altro ente composto direttamente o indirettamente di persone fisiche e dotato o meno di personalità giuridica; infine, uno Stato può comunicare che la convenzione si applichi anche a collezioni di dati non elaborati in forma automatica[220]. In base a quanto previsto dall'articolo 4, ciascuna parte si impegna ad adottare, all'interno del proprio ordinamento, le norme giuridiche necessarie al fine di dare attuazione ai principi fondamentali sanciti nella Convenzione, non prevedendo, però, che tali diritti siano tutelabili in maniera effettiva di fronte ad un tribunale internazionale[221].

Il nucleo fondamentale della Convenzione è rappresentato dal secondo capitolo (articoli 5-10), in cui vengono sanciti i principi fondamentali che ogni Stato si impegna a rispettare in materia di protezione dei dati personali. In particolare, viene in rilievo il principio della "qualità dei dati", in base al quale questi devono essere ottenuti ed elaborati lealmente e legalmente, registrati per fini determinati e legittimi, adeguati, pertinenti e aggiornati, conservati in una forma che permetta l'identificazione delle persone interessate per un periodo non superiore a quello necessario per i fini per i quali essi sono registrati. Una specifica disciplina è invece prevista all'articolo 6 per la categoria dei dati sensibili, i quali possono essere raccolti ed elaborati solo in presenza di presenza di idonee garanzie[222]. Questi sono i dati relativi alle "origini razziali e opinioni politiche, le

[220] Articolo 3, Convenzione 108/1981.
[221] Cfr. L. A. BYGRAVE, *International Agreements to protect personal data, in Global Privacy Protection*, edited by James B. Rule, Edward Elgar Publishing 2008, pag. 22.
[222] Articolo 6 Convenzione 108/1981 "I dati a carattere personale che rivelano l'origine razziale, le opinioni politiche, le convinzioni religiose o altre convinzioni, nonché i dati a carattere personale relativi alla salute o alla vita sessuale, non possono essere elaborati automaticamente a meno che il diritto interno preveda delle garanzie appropriate. Lo stesso vale per i dati a carattere personale relativi a condanne penali".

convinzioni religiose o altri credo, nonché i dati a carattere personale relativi allo stato di salute ed alla vita sessuale".

Altrettanto importanti sono il "principio di sicurezza" sancito all'articolo 7, in base al quale il titolare dell'archivio informatizzato deve adottare misure idonee per proteggere i dati personali dalla distruzione accidentale e non autorizzata, dalla perdita accidentale, nonché dall'accesso, modificazione o diffusione non autorizzati. L'articolo 8 (principio di trasparenza) enuncia due diversi sotto-principi, ossia il diritto del soggetto interessato di venire a conoscenza dell'esistenza di un archivio automatico di dati, delle sue finalità, nonché delle generalità del soggetto che ne è titolare e il diritto di accesso ai dati, di ricevere conferma, secondo determinate modalità, dell'esistenza di un archivio di dati relativi al soggetto interessato e la comunicazione di tali dati in una forma intellegibile.

È infine previsto all'articolo 8, lettera c), il "diritto alla rettifica e cancellazione": il soggetto interessato ha sempre diritto di ottenere la rettifica e la cancellazione dei dati a lui relativi nel caso in cui questi siano stati o siano trattati con modalità non conformi agli articoli 5 e 6 Convenzione, ossia non siano stati rispettati i principi relativi alla qualità dei dati e le particolari tutele a garanzia dei dati sensibili (Articolo 8, lettera d). "Diritto ad un rimedio effettivo": se il soggetto interessato non ha ottenuto soddisfazione ad una delle richieste inoltrate in base ai diritti allo stesso riconosciuti dalle lettere b) e c), ha diritto di avvalersi di una procedura di ricorso.

Per quel che interessa il presente oggetto di indagine, l'articolo 9 della Convenzione prevede che uno Stato possa derogare alle disposizioni in essa contenute quando la limitazione "costituisca una misura necessaria, in una società democratica: a) Per la protezione dello Stato, della sicurezza pubblica, degli interessi monetari dello Stato o per la repressione dei reati; b) Per la protezione della persona interessata e dei diritti e delle libertà di altri". Inoltre, in base a quanto disposto dal paragrafo 3, possono essere apposte delle restrizioni all'esercizio del diritto ad essere informati sul trattamento automatizzato dei propri dati, oppure al diritto di rettifica o cancellazione, quando i dati sono utilizzati per fini statistici o di ricerca scientifica, "allorché chiaramente non vi sia rischio di pregiudizio alla vita privata delle persone interessate"[223].

Occorre sottolineare che la Convenzione è stata recentemente emendata, al fine di modernizzarla ed adattarla ai cambiamenti tecnologici posti in essere negli ultimi anni. La

[223] Articolo 9, par. 3, Convenzione 108/1981.

Convenzione, si ricordi ancora una volta, è l'unico strumento giuridico internazionale vincolante in materia di privacy e protezione dei dati personali applicabile sia ai soggetti privati che pubblici, incluse le autorità di polizia e sicurezza. Durante l'Assemblea plenaria del 27 e 30 dicembre 2012 il Comitato consultivo previsto dall'articolo 18 della Convenzione ha presentato una proposta di modernizzazione della Convenzione, successivamente finalizzata da una commissione nominata *ad hoc* (CAHDATA) e, infine, trasmessa nel giugno 2016 al Comitato dei Ministri.

Tra le maggiori novità introdotte rispetto alla versione originaria, vengono in rilievo, innanzitutto, una maggiore attenzione alla tutela dei dati personali, senza alcuna differenziazione in base alla nazionalità e al luogo di residenza. Inoltre, in linea con quanto previsto anche dal cosiddetto "Pacchetto protezione dati" europeo, la proposta di emendamenti prevede una serie di nuovi obblighi per rinforzare la tutela della privacy, quali, per esempio, l'accountability, la valutazione dell'impatto sulla privacy e il concetto "privacy by design". Essa prevede, infine, alcune nuove disposizioni che rinforzano i diritti in capo alle persone fisiche e misure per rinforzare ed assicurare l'applicazione della Convenzione a livello internazionale[224], anche attraverso la previsioni di autorità di controllo indipendenti ed imparziali.

2.2.3 La Raccomandazione n. R (87) regolante l'utilizzo dei dati personali nel settore di polizia.

In seguito all'adozione della Convenzione 108, il Consiglio dei Ministri ha redatto una serie di raccomandazioni, di natura non vincolante, volte a precisare e adattare i principi enunciati nella Convenzione ai diversi settori in cui i dati personali vengono di volta in volta trattati[225].

---

[224]Cfr. G. VERHENNEMAN, F. COUDERT, *Widening and strengthening the appeal of Convention 108*, in *Data Protection Law & Policy* 2015, pagg. 8-10.

[225]Le raccomadazioni sono in tutto undici: CoE Committee of Ministers, *Recommendation No R (85) 20 on the protection of personal data used for the purposes of direct marketing, 25.10.1985; Recommendation No R (86) 1 on the protection of personal data for social security purposes, 23.01.1986; Recommendation No R (87) 15, cit.; Recommendation No R (89) 2 on the protection of personal data used for employment purposes, 18.01.1989; Recommendation No R (90) 19 on the protection of personal data used for payment and other operations, 13.09.1990; Recommendation No R (91) 10 on the communication to third parties of personal data held by public bodies, 9.09.1991; Recommendation No R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7.02.1995; Recommendation No R (97) 5 on the protection of medical data, 13.02.1997 (*che ha sostituito la precedente *Recommendation no R (81) 1 on regulations for automated medical banks, 23.01.1981); Recommendation No R (97) 18 on the protection of personal data collected and processed for statistical purposes, 30.09.1997 (*che ha sostituito la *Recommendation No R (83) 10 on the protection of personal data used for scientific*

In materia di protezione dei dati personali rileva, in particolare, la Raccomandazione n. R (87) regolante il loro utilizzo nel settore di polizia. Lo scopo di questo strumento giuridico è infatti quello di definire ed uniformare le legislazioni dei vari Stati membri in materia di raccolta, registrazione ed utilizzazione automatizzata dei dati personali per ragioni di pubblica sicurezza[226]. La disciplina speciale, che deroga al regime ordinario previsto dalla Convenzione 108 grazie al rinvio alla "protezione della sicurezza nazionale" operato dall'articolo 9, paragrafo 2, pur prevedendo modalità di trattamento dei dati più invasive rispetto agli *standard* minimi garantiti dall'articolo 8 CEDU, rientra nelle ipotesi di limitazione legittima al diritto previste dal paragrafo 2 dell'articolo stesso.

Passando poi, brevemente, al contenuto sostanziale del testo normativo, nell'articolo 1, paragrafo 1, viene sancito il principio fondamentale, già richiamato in termini generali dalla Convenzione 108, della "supervisione di un'autorità di controllo indipendente", la quale ha il compito di vigilare sul rispetto dei principi enunciati nella Raccomandazione. In base a quanto previsto dalla normativa in esame, l'attività di supervisione dovrebbe essere attuata, principalmente, stabilendo in capo al soggetto titolare dell'archivio dei dati presso un'autorità di polizia l'obbligo "di consultare preventivamente l'autorità di controllo ogni qualvolta l'introduzione di procedimenti di trattamento automatizzato sollevi interrogativi riguardanti l'attuazione della presente raccomandazione"[227]. La supervisione dovrebbe essere inoltre garantita attraverso l'obbligo di notifica all'autorità di controllo del possesso di archivi automatizzati, con l'indicazione, in particolare, dell'organo responsabile del trattamento, della specifica natura dei dati, nonché della loro finalità e dei loro destinatari[228].

Altri principi importanti enunciati dalla Raccomandazione sono quelli della "proporzionalità" e "necessità". In particolare, ai sensi dell'articolo 2, par. 1, la raccolta dei dati dovrebbe essere limitata a quanto strettamente necessario per prevenire un "pericolo

---

research and statistics, 23.09.1983); Recommendation No R (99) 5 for the protection of privacy on the Internet, 23.02.1999); infine, la *Recommandation No R (2002) 9 on the protection of personal data collected and processed for insurance purposes, 18.09.2002.* Ogni raccomandazione è accompagnata dal relativo *memorandum* esplicativo.

[226]Nel testo della Raccomandazione viene specificato che cosa si intenda con l'espressione "a fini di pubblica sicurezza": l'insieme dei compiti che ricadono sulle autorità di pubblica sicurezza per la prevenzione e la repressione dei reati penali e per il mantenimento dell'ordine pubblico.

[227]Articolo 1, paragrafo 3 Raccomandazione n. R (87), disponibile alla pagina http://194.242.234.211/documents/10160/10704/CONSIGLIO+D'EUROPA+RACCOMANDAZIONE+N.+R+%2887%29.

[228] *Ibidem,* paragrafo 4.

concreto", ovvero per reprimere uno specifico crimine. Inoltre, qualsiasi misura di deroga deve essere prevista specificatamente dalla legge. Viene poi in rilevo il "principio di non discriminazione", in base al quale le informazioni personali di tipo "sensibile" - ossia quelle concernenti l'origine razziale, determinate convinzioni religiose, comportamenti sessuali o opinioni politiche di un individuo - possono essere raccolte solo quando strettamente necessarie per una specifica inchiesta. Infine, vengono in rilievo i principi di adeguatezza della raccolta dei dati, della finalità predeterminata del trattamento, della circolazione dei dati, nonché del diritto di rettifica, cancellazione e rimedio in capo al soggetto interessato. Viene enunciato, infine, il principio della sicurezza dei dati.

2.3 LA CONVENZIONE AMERICANA SUI DIRITTI UMANI E LA CARTA ARABA DEI DIRITTI UMANI

Si rende infine opportuno menzionare, per necessità di completezza con riferimento al quadro giuridico sopra delineato in materia di tutela della privacy, che la Convenzione americana sui diritti umani, adottata il 22 novembre 1969 a San José in Costarica ed entrata in vigore il 18 luglio 1978, prevede all'articolo 11 che: "1. Ognuno ha il diritto a che il proprio onore e reputazione siano riconosciuti. 2. Nessuno può essere soggetto ad interferenze arbitrarie o abusive nella vita privata, nella famiglia, nel domicilio, o nella corrispondenza, oppure ad illegittimi attacchi al proprio onore o reputazione. 3. Ognuno ha il diritto alla tutela giuridica contro ogni interferenza o attacco"[229].

Dato il contesto storico, economico e sociale in cui la Convenzione americana sui diritti umani è stata adottata, ma soprattutto quello in cui la Corte interamericana e Commissione interamericana ancora oggi operano - che rendono necessari interventi legislativi e giurisprudenziali su temi più contingenti quali il rispetto alla vita e alla dignità umana e il divieto di tortura – non si rilevano finora significativi interventi in materia di protezione dei dati personali. Ciononostante, sembra che l'interesse verso una maggior tutela della privacy abbia iniziato manifestarsi negli ultimi anni con maggiore insistenza anche nel continente latino-americano, com'è stato d'altronde dimostrato dal recente

[229]Traduzione letterale ad opera dell'autore. Il diritto alla riservatezza viene tutelato inoltre dall'articolo V della Dichiarazione americana, (American Declaration of the Rights and Duties of Man) a menzione del quale "[a]ll persons have the right to protection of the Law against abusive attacks on their honor, their reputation and their private and family life" and Article X establishes that "all persons have the right to the inviolability and circulation of their correspondence".

rapporto sugli *Standard for a Free, Open and inclusive Internet* pubblicato il 15 marzo 2017[230]. In particolare, ivi è stato evidenziato come "The development of the Internet empowers and simplifies communications and the storage and standardization of information. But it also empowers States and private parties to more easily conduct monitoring, collection, and surveillance of data, representing a serious risk to privacy[231]". Malgrado ciò, ad oggi la disciplina sulla suddetta materia continua ad essere scarna e frammentaria.

Per quanto riguarda la Convenzione interamericana, le limitazioni al diritto alla privacy possono ricavarsi in maniera implicita, alla pari di quanto previsto dall'articolo 17 del Patto sui diritti civili e politici, dal fatto che ai sensi dell'articolo 11 le interferenze nella vita privata non devono essere *arbitrarie* o *abusive*, ammettendole quindi quando sono giustificate e legittime[232].

Un'analoga disposizione è prevista anche all'articolo 17 della Carta araba dei diritti umani, adottata il 15 settembre 1994 dal Consiglio della Lega Araba ed emendata poi nel 2004 in occasione del Summit della Lega araba. Essa è entrata in vigore solo nel 2008.
Il summenzionato articolo prevede, infatti, che "Privacy shall be inviolable and any infringement thereof shall constitute an offence. This privacy includes private family affairs, the inviolability of the home and the confidentiality of correspondence and other private means of communication".

[230]Commissione interamericana dei diritti umani, *Standard for a Free, Open and inclusive Internet,* 15 marzo 2017, OEA/Ser.L/V/II CIDH/RELE/INF.17/17.
[231]*Ibidem*, punto 184.
[232]Cfr. S. DAVIDSON, *The Civil and Political Rights Protected in the Inter-American Human Rights System*, in D. J. HARRIS, S. LIVINGSTONE, *The Inter-american System of Human Rights,* Oxford University Press, 1998, pag. 256.

CAPITOLO 3
IL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI NELLA GIURISPRUDENZA DELLA CORTE DI GIUSTIZIA DELL'UNIONE EUROPEA E DELLA CORTE EUROPEA DEI DIRITTI UMANI

3.1 L'APPROCCIO DELLA CORTE DI GIUSTIZIA 3.1.1 La dottrina del margine di apprezzamento 3.2 L'APPROCCIO DELLA CORTE EUROPEA DEI DIRITTI UMANI 3.2.1 La dottrina del margine di apprezzamento 3.2.2 Il principio di proporzionalità 3.2.3 Lo *status* di vittima 3.2.4 Il controllo giurisdizionale e l'obbligo di notifica 3.2.5 Il test della necessità. 3.2.6 La separazione tra il potere giudiziario e il potere legislativo 3.3 VERSO UN SISTEMA EUROPEO UNIFORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Nel primo e nel secondo capitolo è stato analizzato il diritto alla protezione dei dati personali in astratto delineando, in termini generali, sia la sua evoluzione storica che le principali fonti del diritto internazionale ed europeo.

In questa parte dell'elaborato verrà, invece, trattato il problema della tutela della privacy in concreto, mettendo in evidenza alcuni degli aspetti più critici emersi nelle recenti pronunce della Corte europea dei diritti umani e della Corte di giustizia dell'Unione europea in materia di sorveglianza di massa e della possibilità riconosciuta agli Stati di limitare i diritti per ragioni di sicurezza nazionale ed esigenze di *law enforcement*. Anche in questo contesto sembrerebbe, infatti, andandosi sviluppando quello che molti in dottrina chiamano il cosiddetto "dialogo fra le due Corti"[233] reso ancora più evidente dal ricorrere di alcuni concetti comuni quale il principio di proporzionalità e quello di necessità. Invero, è proprio sulla base di questi concetti che i giudici di Lussemburgo e Strasburgo hanno delineato i limiti dell'agire delle autorità di pubblica sicurezza e polizia in materia di protezione dei dati personali e misure di intercettazione. Il diritto alla privacy deve essere tutelato, oltre che nei confronti dello Stato membro di cui l'individuo è cittadino, anche nei confronti di possibili violazioni provenienti da Paesi terzi. Questo ha portato ad un rafforzamento del diritto tale per cui "so far, this development seems to be unquestioned by national courts"[234].

A livello strettamente legislativo, nella precedente direttiva 95/46/CE, e nuovamente richiamato ora anche nel nuovo regolamento (UE) 2016/679[235], viene indicato all'articolo 1 come obiettivo principale da raggiungere attraverso il testo normativo, quello di garantire "[…] la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla vita privata, con riguardo al trattamento dei dati personali". Secondo alcuni,

[233]Cfr. O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?,* in *Forum di Quaderni costituzionali*, 31 dicembre 2013, pagg. 1-27.
[234]F. BOEHM, *Assessing the New Instruments in EU-US Data Protection Law*, in *European Data Protection Law Review*, 2016, pag. 179.
[235]Articolo 1, par. 2, regolamento (UE) 2016/679 "Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali".

l'enfasi apposta sul bisogno di tutelare i diritti e le libertà fondamentali delle persone fisiche costituirebbe la prova di un primordiale collegamento fra la suddetta fonte europea e l'articolo 8 CEDU, reso ancora più evidente dopo il Trattato di Lisbona e il riconoscimento dell'articolo 8 della Carta di Nizza della tutela dei dati personali quale diritto fondamentale dell'Unione europea.

Dal punto di vista strutturale, il capitolo verrà articolato nella seguente maniera. Verranno analizzati, in *primis,* i casi *Digital Rights Ireland Ltd* [236] e *Maximilian Schrems*[237] decisi dalla Corte di giustizia con i quali sono state rispettivamente invalidate la direttiva 2006/24/CE relativa ai servizi di comunicazione elettronica e il cosiddetto pacchetto "Safe Harbour". Si farà inoltre accenno alle problematiche sottese al parere reso dalla Corte di giustizia in merito all'accordo PNR tra Unione europea e Canada. Successivamente, ci si soffermerà, invece, sulle sentenze *Roman Zakharov c. Russia* e *Szabo e Vissy c. Ungheria* della Corte europea dei diritti umani. Appare evidente in queste due pronunce il costante richiamo alla giurisprudenza di Lussemburgo, soprattutto alla recente sentenza *Digital Rights Ireland Ltd*, anche alla luce del fatto che l'Ungheria è anche un Paese membro dell'Unione europea e che entrambe le sentenze hanno affrontato il problema della sorveglianza di massa[238]. Allo stesso modo, diversi sono i richiami operati nel caso *Digital Rights Ireland Ltd* alle sentenze della Corte europea dei diritti umani, quali, per esempio, *Rotaru c. Romania*[239], *Liberty e altri c. Regno Unito*[240], *S. e Marper c. Regno Unito*[241] con riferimento, soprattutto, al giudizio di proporzionalità[242].

In secondo luogo, verranno messe in evidenza le principali problematiche identificate negli esposti casi giurisprudenziali, soffermandosi, in particolare, sui problemi legati allo *status* di vittima, necessario per proporre legittimamente ricorso ai sensi dell'articolo 34 CEDU, e sulla carenza a livello legislativo nazionale di adeguate misure di

[236]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd,* cit.
[237]Corte di giustizia dell'Unione europea (Grande Sezione), *Maximilian Schrems,* cit.
[238]Cfr. M. D. COLE, A. VANDENDRIESSCHE, *From Digital Rights Irland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in *European Data Protection Law Review* 2016, pag. 127. I riferimenti sono presenti, seppur in maniera meno rilevante, anche nella sentenza della Corte europea dei diritti umani (GC) *Roman Zakharov* c. *Russia,* cit., par. 147.
[239]Corte europea dei diritti umani, *Rotaru c. Romania*, sentenza del 4 maggio 2000, ricorso n. 28341/95.
[240]Corte europea dei diritti umani, *Liberty e altri c. Regno Unito*, sentenza del 1 luglio 2008, ricorso n. 58243/00.
[241]Corte europea dei diritti umani (GC), *S. e Marper c. Regno Unito*, cit.
[242]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., parr. 47 e 54.

controllo giurisdizionale preventivo e successivo e di istituti a tutela del singolo come l'obbligo di notifica *ex post* in caso di violazione da parte delle autorità statali.

Infine, la terza parte del capitolo sarà dedicata alla trattazione degli principi comuni richiamati sia dalla Corte di giustizia sia dalla Corte europea dei diritti umani, cercando di delineare la struttura di quello che potrebbe essere definito il sistema uniforme di tutela del diritto alla protezione dei dati personali nel contesto europeo.

3.1 L'APPROCCIO DELLA CORTE DI GIUSTIZIA

A livello giurisprudenziale europeo, la Corte di giustizia ha manifestato negli ultimi anni un crescente interesse nei confronti della tutela della privacy/dati personali, pronunciandosi, in particolare, con ben quarantaquattro pronunce[243], di cui dieci decise composizione Grande Sezione[244].

Per quel che concerne il presente oggetto di indagine, la prima sentenza che viene in rilievo è il caso *Digital Rights Ireland Ltd*[245], con il quale è stata invalidata la direttiva 2006/24/CE relativa ai servizi di comunicazione elettronica[246] in quanto contrastante con i diritti sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione, che tutelano, rispettivamente, la vita privata e familiare e i dati personali. Invero, in base alla summenzionata direttiva i *provider* di comunicazioni elettroniche avevano l'obbligo di

[243]Le sentenze sono disponibili sul sito della Corte di giustizia, www.curia.eu, inserendo le parole chiave "Data Protection". E' stato inoltre redatto dall'Ufficio del DPO in collaborazione con l'Ufficio OLAF un rapporto disponibile al sito https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf.

[244]Le sentenze della Corte di giustizia sono le seguenti: (Grande Sezione) *Maximilian Schrems c. Data Protection Commissioner*, cit.; (Grande Sezione) *Digital Rights Ireland Ltd*, cit.; *Commissione c. Ungheria*, sentenza dell'8 Aprile 2014, causa C-288/12; (Grande Sezione) *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 Maggio 2014, causa C-131/12; *Commissione Europea c. Austria*, sentenza del 16 Ottobre 2012, causa C-614/10; (Grande Sezione) *Volker Volker und Markus und Markus Schecke GbR, Hartmut Eifert c. Land Hessen*, sentenza del 9 Novembre 2010, cause riunite C-92/09 e C-93/09; (Grande Sezione) *Commissione Europea c. The Bavarian Lager Co. Ltd*, sentenza del 29 Giugno 2010, causa C-28/08; (Grande Sezione) *Heinz Huber c. Germania*, sentenza del 16 Dicembre 2008, causa C-524/06; (Grande Sezione) *Productores de Música de España (Promusicae) v Telefónica de España SAU*, sentenza del 29 Gennaio 2008, causa C-275/06; *Parlamento Europeo c. Consiglio dell'Unione europea e Parlamento europeo c. Commissione delle Comunità europee*, sentenza del 30 maggio 2006, cause reunite C-317/04 e C-318/04.

[245]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd,* cit.

[246]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.

conservare i dati personali, per finalità di sicurezza nazionale, per un periodo non inferiore a sei mesi e non superiore ai due anni[247].

Al riguardo, la Corte di giustizia ha evidenziato come la conservazione dei dati relativi agli utenti registrati per un periodo compreso fra sei mesi e due anni, e la loro conseguente utilizzazione senza che i soggetti interessati ne fossero informati, comportasse il rischio di una costante ingerenza nella vita privata e familiare di pressoché tutta la popolazione europea[248]. La direttiva 2006/24/CE , inoltre, nonostante fosse finalizzata a reprimere i reati più gravi e a contrastare il terrorismo internazionale, non era sufficientemente dettagliata né sotto il profilo dell'indicazione dei criteri necessari per l'adozione delle suddette misure di sorveglianza, né sotto quello della durata e dei destinatari delle stesse[249]. Essa interessava infatti tutti gli individui e tutti i tipi di comunicazione elettronica, senza che fosse operata una distinzione tra le varie categorie di soggetti e senza che fosse, soprattutto, necessario fornire la prova di un collegamento, o quanto meno di un ragionevole sospetto, che quel determinato individuo avesse commesso un reato[250]. Inoltre, non erano sufficientemente indicati i criteri in base ai quali ritenere un reato così grave da giustificare una misura di interferenza[251]. La misura limitativa al diritto alla protezione dei dati personali non era pertanto proporzionata e necessaria rispetto alle finalità perseguite e non prevedeva, inoltre, sufficienti garanzie in capo agli individui per proteggersi contro eventuali abusi[252]. Con riferimento, in particolare, al principio di necessità, i giudici di Lussemburgo ribadivano che, secondo costante giurisprudenza europea, fosse necessario che "[…]le deroghe e le restrizioni alla tutela dei dati personali [dovessero[253]] operare entro i limiti dello stretto necessario"[254].

L'orientamento espresso dalla Corte di giustizia in questa pronuncia è stato poi ulteriormente confermato nel successivo caso *Maximilian Schrems c. Data Protection Commission*[255]*,* ove è stato invalidato il cosiddetto pacchetto commerciale "Safe

[247]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., par. 16.
[248]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., par. 37.
[249]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., parr. 56-64. In dottrina cfr. G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, in *Roma TrE-PRESS*, Roma 2016, pag. 41.
[250]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., parr. 58.
[251]*Ibidem,* par. 60.
[252]*Ibidem*, par. 61.
[253]Parentesi aggiunta.
[254]*Ibidem*, par. 52.
[255]Corte di giustizia (Grande Sezione), *Maximilian Schrems,* cit.. Cfr. in dottrina G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems* in *La*

Harbour"[256]. La *querelle* giudiziaria promossa dal giovane attivista austriaco riguardava il suddetto accordo internazionale, stipulato tra Unione europea e Stati Uniti, che permetteva di fatto il flusso indiscriminato di informazioni da una parte all'altra dell'Oceano. Il ricorrente aveva infatti appreso, dopo un periodo di studi trascorso negli Stati Uniti[257], che i dati personali degli utenti del noto *social network* Facebook venivano raccolti nella sede irlandese e venivano poi direttamente trasmessi negli Stati Uniti, ove era noto che, anche a causa delle concomitanti rivelazioni di Snowden sui programmi di sorveglianza di massa come il PRISM, il diritto alla privacy non riceveva una sufficiente tutela.

Schrems presentava inizialmente denuncia alle autorità irlandesi di controllo (*Data Protection Commissioner)*, le quali rigettavano la sua istanza in ragione del fatto che la Commissione europea aveva dichiarato nel 2000 che, nel contesto dell'accordo "Safe Harbour", gli Stati Uniti assicuravano un livello di protezione adeguato ai dati trasferiti dall'Unione europea verso il continente americano[258].

Adita in appello la *High Court*, questa investiva a sua volta della causa la Corte di giustizia dell'Unione europea chiedendo, come questione pregiudiziale, se una decisione della Commissione, con la quale essa dichiarava che la normativa di un Paese terzo verso il quale i dati dei cittadini europei venivano trasferiti garantiva un adeguato livello di tutela, non impedisse alle autorità nazionali di decidere a loro volta sulla questione in piena autonomia, in ragione del potere di cui godevano in forza della Carta dei diritti fondamentali dell'Unione europea. Alla risposta veniva fornita risposta positiva[259] e la Corte stabiliva, inoltre, che, nel caso in cui suddette autorità avessero respinto le richieste

---

protezione transnazionale dei dati personali, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, Roma TrE-PRESS, Roma 2016; Cfr. M. BASSINI, O. POLLICINO, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo,* in *La protezione transnazionale dei dati personali*, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, Roma TrE-PRESS, Roma 2016, pagg. 113-135 e 73-113.

[256]L'accordo era stato ritenuto valido con la decisione della Commissione Europea 2000/520/EC del 26 luglio 2000.

[257]In quell'occasione l'allora studente di giurisprudenza Maximilian Schrems aveva richiesto alla sede principale del social network di Cupertino (U.S.A.) lo storico di tutti i dati personali raccolti dalla società relativi al suo account e aveva ricevuto un file contenenti migliaia di pagine relative anche ad informazioni ed immagini che egli aveva precedentemente cancellato.

[258]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, 25 agosto 2000, GU L. 215/7.

[259]Corte di giustizia (Grande Sezione), *Maximilian Schrems,* cit., par. 63.

presentate dai singoli, questi avrebbero potuto rivolgersi ai giudici nazionali, i quali, a loro volta, avrebbero potuto investire della causa la Corte di giustizia[260].

Il 6 ottobre 2015 la Corte di giustizia dichiarava quindi invalida la decisione della Commissione europea del 2002 che aveva dichiarato l'idoneità del cosiddetto pacchetto "U.S. Safe Harbour", dal momento che questo, non garantendo un adeguato livello di protezione ai cittadini europei, si poneva in contrasto con gli articoli 7[261], 8[262] e 47[263] della Carta dei diritti fondamentali dell'Unione europea, nonché con gli articoli 25, paragrafo 6[264], e 28 della direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali[265]. Invero, oltre ai rischi connessi all'utilizzo su larga scala dei dati personali da parte dell'NSA e di altri organi federali come il *Federal Bureau of Investigation* (FBI)[266], nella pronuncia in esame la Corte di giustizia evidenziava la mancanza in capo ai cittadini europei di strumenti volti ad ottenere la rettifica o la cancellazione delle informazioni ottenute nell'ambito dei suddetti programmi di controllo statunitensi[267]. Il trasferimento dei dati per finalità commerciali era reso possibile grazie al sopramenzionato accordo internazionale, altrimenti detto sistema di "approdo sicuro", costituito da un insieme di principi e di linee guida cui le società statunitensi potevano liberamente aderire, semplicemente presentando un'autocertificazione con quale

[260]*Ibidem*, par. 64.
[261]Articolo 7 Carta dei diritti fondamentali dell'Unione europea: "Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni".
[262]Articolo 8 Carta dei diritti fondamentali dell'Unione europea: "1.Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente".
[263]Articolo 47 Carta dei diritti fondamentali dell'Unione europea: "Ogni individuo i cui diritti e le cui libertà garantiti dal diritto dell'Unione siano stati violati ha diritto a un ricorso effettivo dinanzi a un giudice, nel rispetto delle condizioni previste nel presente articolo. Ogni individuo ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un giudice indipendente e imparziale, precostituito per legge. Ogni individuo ha la facoltà di farsi consigliare, difendere e rappresentare. A coloro che non dispongono di mezzi sufficienti è concesso il patrocinio a spese dello Stato qualora ciò sia necessario per assicurare un accesso effettivo alla giustizia.
[264]Articolo 25, paragrafo 6, direttiva 95/46/CE "La Commissione può constatare, secondo la procedura di cui all'articolo 31, paragrafo 2, che un paese terzo garantisce un livello di protezione adeguato ai sensi del paragrafo 2 del presente articolo, in considerazione della sua legislazione nazionale o dei suoi impegni internazionali, in particolare di quelli assunti in seguito ai negoziati di cui al paragrafo 5, ai fini della tutela della vita privata o delle libertà e dei diritti fondamentali della persona".
[265]Articolo 28 direttiva 95/46/CE.
[266]Corte di giustizia (Grande Sezione), *Maximilian Schrems,* cit. par. 31.
[267]Recentemente, inoltre, la Suprema Corte Irlandese ha proposto rinvio pregiudiziale alla Corte di giustizia con riferimento al cosiddetto caso Schrems II, concernente la validità delle clausole contrattuali standard ("SCCs") che facilitano il trasferimento dei dati personali verso paesi non membri dell'Unione europea.

dichiaravano di essere a conoscenza del suo contenuto e di impegnarsi a rispettare i principi in esso sanciti[268].

Il suddetto sistema presentava, però, due grandi problematiche. In primo luogo, il suo ambito di applicazione era limitato solo alle imprese private americane che lo sottoscrivevano e non veniva, invece, esteso anche alle pubbliche autorità. In secondo luogo, le società americane erano tenute a disapplicare le tutele previste dagli accordi tutte le volte in cui venivano in gioco esigenze di sicurezza nazionale e pubblica necessità. Queste ultime prevalevano, infatti, sempre su quelle di natura commerciale.

Invero, già prima della Corte di giustizia, anche la Commissione europea aveva manifestato, in due comunicazioni rivolte al Parlamento europeo e al Consiglio e datate al 27 novembre 2013, le proprie perplessità in merito alla compatibilità delle clausole di limitazione per ragioni di sicurezza nazionale con i principi di necessità e proporzionalità[269], dal momento che, anche secondo costante giurisprudenza della Corte, tutte le limitazioni al summenzionato diritto dovevano sempre essere interpretate in maniera restrittiva[270]. In entrambe le comunicazioni era stato inoltre evidenziato come tutte le imprese coinvolte nel programma PRISM relativo alla sorveglianza di massa risultassero certificate nell'accordo di approdo sicuro e questo aveva fatto sì che i dati personali dei cittadini europei fossero quindi accessibili alle autorità di sicurezza americana e utilizzati per finalità diverse da quelle originarie, di natura strettamente commerciale, che avevano giustificato il loro trasferimento negli Stati Uniti[271]. Alle stesse conclusioni giungeva anche

---

[268]Cfr. V. SALVATORE, *La Corte di Giustizia restituisce (temporaneamente) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti,* in *Studi sull'integrazione europea,* 2015, pag. 627. Cfr. anche X. TRACOL, "*Invalidator" strikes back: The harbour has never been safe*, in *Computer Law and Security Review,* 2016 pp. 345-362.

[269]Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, Bruxelles, 27 novembre 2013, COM/2013/846 final, pag. 4; Comunicazione della Commissione al Parlamento europeo e al Consiglio, *sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite*, Bruxelles 27 novembre 2013, COM/2013/847 final, pagg. 17 e 18.

[270]Sentenze della Corte di giustizia a riguardo: *Rechnungshof c. Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann c. Österreichscher Rundfunk*, sentenza del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01; (Grande Sezione) *Productores de Música de España (Promusicae)*, cit.; (Grande Sezione) *Volker e Markus Schecke GbR, Hartmut Eifert,* cit. In dottrina cfr. K. IRION, *A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection,* in U. FABER, K. FELDHOFF, K. NEBE, K. SCHMIDT, U. WASSER (HRSG), *Gesellschaftliche Bewegugen-Recht unter Beobachtung und in Aktion,* Nomes, Baden Baden 2016, pag. 882.

[271]Comunicazione della Commissione al Parlamento europeo e al Consiglio, *Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA*, Bruxelles 27 novembre 2013, COM/2013/846 final, pag. 4; Comunicazione della Commissione al Parlamento europeo e al Consiglio, *sul funzionamento del regime*

il Parlamento europeo in una risoluzione del 2014[272] - cui faceva seguito un'altra di aggiornamento l'anno successivo - con la quale esso, denunciati i programmi di sorveglianza attuati negli Stati Uniti che avevano coinvolto e danneggiato anche i diritti fondamentali dei cittadini europei[273], invitava la Commissione a sospendere la decisione 2000/520/CE con la quale era stato validato l'accordo e a ridefinire i relativi accordi con gli Stati Uniti[274].

Si noti bene, nella sentenza *Maximilian Schrems* la Corte di giustizia volontariamente omette un giudizio in merito al livello di protezione offerto dal sistema legislativo americano al fine di stipulare accordi in materia di flussi di dati con l'Unione europea – la cosiddetta "adequacy decision", che interviene tutte le volte in cui gli Stati terzi fanno richiesta di ricevere dati personali provenienti dall'Unione europea senza restrizioni, ora prevista dall'articolo 45, par. 1, del regolamento (UE) 2016/679 – ma si limita a dire che l'accordo "Safe Harbour" è invalido perché non conforme ai diritti sanciti dalla Carta dei diritti fondamentali dell'Unione europea e dalla direttiva 95/46/CE in materia di protezione dei dati personali. In particolare, viene constatato che "[…]legislation is not limited to what is strictly necessary where it authorises, on a generalised basis, storage of all personal data of all the persons whose data has been transferred from the (EU) to the (US) without any differentiation, limitation or exception being made in the light of the objective pursued and without any objective criterion being laid down by which to determinate the limits of the access of the public authorities to the data, and of its subsequent use…[…]"[275]. Secondo i giudici di Lussemburgo, infatti, lo Stato terzo deve garantire che la raccolta e l'utilizzo dei dati personali per finalità di

"Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite, Bruxelles 27 novembre 2013, COM/2013/847 final, pag. 17.

[272]Relazione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugli organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni, 21 febbraio 2014, 2013/2188(INI), parr. 35 e 36.

[273]Risoluzione del Parlamento europeo del 29 ottobre 2015 sul seguito dato alla risoluzione del Parlamento europeo del 12 marzo 2014 sulla sorveglianza elettronica di massa dei cittadini dell'Unione (2015/2635(RSP)), considerando A.

[274]*Ibidem,* parr. 39 e 41. Analoghe preoccupazioni erano state espresse anche dall*'Article 29 Working Party (*WP29, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 10 aprile 2014, 819/14/EN WP 215), e dal Garante europeo per la Protezione dei dati, con un parere sulla comunicazione della Commissione al Parlamento europeo e al Consiglio «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle aziende ivi stabilite, il 16 aprile 2014, 2014/C 116/04 (disponibile alla pagina: https://edps.europa.eu/sites/edp/files/publication/14-02-19_eu_us_rebuliding_trust_ex_sum_it.pdf).

[275]Corte di giustizia (Grande Sezione), *Maximilian Schrems*, cit., par. 93.

intelligence e di sicurezza nazionale avvenga nel rispetto del principio di proporzionalità, sia limitato allo specifico scopo da perseguire e si fondi sul ragionevole sospetto che la persona destinataria delle misure di sorveglianza sia in qualche modo coinvolta in attività connesse al terrorismo. Parimenti, è necessario che vengano previsti dei meccanismi giurisdizionali di controllo in capo ai singoli per tutelarlo in caso di violazioni o abusi di potere da parte delle autorità statali [276].

In seguito a tale pronuncia, la Commissione europea, l'Amministrazione svizzera e il Dipartimento americano hanno presentato un nuovo progetto di accordo, denominato "The EU-U.S. Privacy Shield"[277], il quale rinforza i diritti spettanti ai cittadini europei, imponendo degli *standard* di trasparenza più elevanti, maggiori obblighi anche nei confronti delle società private che raccolgono e processano i dati personali, prevedendo dei rimedi in capo agli individui in caso di violazione dei loro dati, e auspicando, infine, una maggiore cooperazione fra le autorità garanti dei diversi Paesi europei tutte le volte in cui i dati personali vengono trasferiti dall'Unione europea o dalla Svizzera verso gli Stati Uniti. Il suddetto accordo è stato oggetto di analisi dell'*Article 29 Working Party* - un organismo indipendente e consultivo istituito dall'articolo 29 della direttiva 95/46/CE a tutela dei dati personali dei cittadini[278] - il quale si è espresso con un parere il 28 novembre 2017[279]. Ivi sono stati rilevati in maniera positiva gli sforzi compiuti dagli Stati Uniti per garantire una maggiore trasparenza delle attività svolte dai servizi di *intelligence* americani. Ciononostante, ci sono ancora diversi aspetti che destano le preoccupazioni dell'*Article 29 Working Party* con riferimento, soprattutto, alle modalità di raccolta dei dati previste sia dalla sezione 702 del Foreign Surveillance Intelligence Act, relativo alla raccolta di informazioni personali e ai programmi di sorveglianza sulle persone al di fuori degli Stati Uniti[280] - il quale non prevede, ad esempio, né il requisito del "ragionevole sospetto" quale condizione per potere applicare una misura di interferenza, né il preventivo controllo

[276]Corte di giustizia (Grande Sezione), *Maximilian Schrems*, cit., par. 95.
[277]Decisione della Commissione europea, 1250/2016/EC del 12 luglio 2016.
[278]L'organismo è composto da un rappresentante delle autorità nazionali, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione. Il regolamento (UE) 2016/679 ha sostituito l'*Article 29 Working Party* con il nuovo *European Data Protection Board*.
[279]Article 29 Working Party, *EU – U.S. Privacy Shield – First annual Joint Review*, 28 novembre 2017, 17/EN, WP 255.
[280]Foreign Intelligence Act, approvato il 25 ottobre 1978, più volte emendato soprattutto in seguito all'11 settembre dall'USA Patrioct Act, con il quale sono state introdotte diverse disposizioni legislative finalizzate alla lotta al terrorismo internazionale, disponibile alla pagina https://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf.

giurisdizionale – sia dall'Executive Order 12333[281] sulle attività di *intelligence*. Inoltre, il sistema legislativo statunitense non prevede sufficienti garanzie in capo agli individui nel caso in cui i dati posseduti dalle società siano raccolti dalle autorità statali per ragioni di *law enforcement*[282]. In base a quanto previsto nel rapporto, i suddetti punti critici dovranno essere risolti entro il 28 maggio 2018, diversamente gli Stati membri saranno liberi di portare la questione nuovamente di fronte alla Corte di giustizia.

Orbene, come si avrà modo di analizzare in seguito, le due sentenze appena analizzate sono state richiamata più volte dalla Corte europea dei diritti umani sia nel caso relativo alle misure di intercettazione russe sia di quelle ungheresi, a riprova dei numerosi elementi di similarità che presentano, rispettivamente, il sistema di tutela dei diritti umani europeo e CEDU.

Viene in rilievo, poi, la sentenza *Tele2 Sverige AB*, resa dalla Corte di giustizia in data 21 dicembre 2016[283]. La questione pregiudiziale riguardava l'obbligo imposto dal diritto svedese e inglese in capo agli fornitori di servizi di comunicazione elettronica di conservare in maniera indiscriminata e continuativa i dati degli utenti, reso possibile grazie alla direttiva europea 2002/58/CE.

I giudici di Lussemburgo constatavano, innanzitutto, che le leggi in esame, le quali consentivano la conservazione dei dati per finalità di contrasto alla criminalità, rientravano nell'ambito di applicazione dell'articolo 15, paragrafo 1, della direttiva europea 2002/58/CE. Ivi veniva prevista infatti la possibilità per gli Stati membri di adottare misure legislative volte a conservare per un periodo limitato i dati, in deroga agli obblighi e ai diritti previsti dagli articoli 5, 6 e 9 della direttiva, al fine di salvaguardare la sicurezza pubblica e nazionale, prevenire, accertare e perseguire i reati. Le suddette misure dovevano essere conformi ai principi di proporzionalità e necessità.

Per quanto riguarda invece la questione pregiudiziale, la Corte riteveneva contraria al diritto dell'Unione europea una normativa nazionale che prevedeva, come nel caso di specie, la conservazione generalizzata ed indifferenziata dei dati, dal momento che essa eccedeva i limiti dello strettamente necessario.

---

[281]Executive Order 12333, United States Intelligence Activities, 4 dicembre 1981, emendato dall'Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008)), disponibile al sito https://www.cia.gov/about-cia/eo12333.html.

[282]*EU – U.S. Privacy Shield – First annual Joint Review*, cit., pag. 4.

[283]Corte di giustizia (Grande Sezione), *Tele2 Sverige AB,* cit.

Sia nel caso *Digital Rights Ireland Ltd* che *Tele2 Sverige AB*, i giudici di Lussemburgo sono stati chiamati a pronunciarsi sulla compatibilità della normativa nazionale con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea e a valutare se le misure di interferenza possano considerarsi necessarie e proporzionate ai fini perseguiti ai sensi dell'articolo 52[284]. Invero, il giudizio relativo alla compatibilità della legislazione statale con quest'ultima norma si differenzia, seppur in maniera marginale, nelle due pronunce analizzate. In particolare, "[…] in *Digital Rights Ireland Ltd*, the Court analysed in details the different conditions under which derogations to the fundamental rights are permitted, whereas in *Tele2 Sverige*, the Court mainly focused on the proportionality of the national laws derogating to the principle of proportionality"[285].

Sempre in materia di tutela della privacy a livello europeo viene in rilievo, infine, il parere del 26 luglio 2017 con cui la Corte di giustizia ha dichiarato invalido l'accordo tra la Comunità europea e il governo canadese sul trattamento delle informazioni anticipate sui passeggeri e dei dati delle pratiche passeggeri ("accordo del 2006") in quanto non compatibile con gli articoli 16 TFUE e 7 e 8 della Carta dei diritti fondamentali dell'Unione europea[286].

Questa è la prima volta in cui la Corte è chiamata a pronunciarsi sulla compatibilità di un progetto di accordo internazionale con i diritti fondamentali sanciti dall'Unione europea e, in particolare, con il diritto alla privacy e alla tutela dei dati personali. Nell'esaminare la questione, essa si rifà principalmente ai principi sanciti delle pronunce *Digital Rights Ireland Ltd* e *Maximilian Schrems*[287], constatando la necessità, in un momento storico in cui le tecnologie sempre più sofisticate vengono utilizzate dalle autorità statali per monitorare i dati personali e la vita degli individui in nome del bisogno di contrastare il terrorismo e la criminalità internazionale, di trovare sempre un giusto bilanciamento tra il bisogno di garantire la sicurezza pubblica e quella di tutelare il diritto alla privacy, equamente degno di tutela.

---

[284]C. JASSERAND, *Law enforcement access to personal data originally collected by private parties:Missing data subject's safeguards in directive 2016/680?,* in *Computer Law & Security Review 2018,* pag. 159.
[285]*Ibidem*, pag. 160.
[286]Corte di Giustizia (Grande Sezione), *Progetto di accordo tra il Canada e l'Unione europea– Trasferimento dei dati del codice di prenotazione dei passeggeri aerei dall'Unione al Canada*, 26 luglio 2017, parere n. 1/15.
[287]*Ibidem,* par. 7.

In particolare, viene rilevata la mancanza di un'indicazione delle categorie di dati cui l'accordo si applica e, conseguentemente, allo stesso sono assoggettati in maniera indiscriminata anche i dati sensibili. Inoltre, non vengono descritte in maniera sufficientemente chiara le finalità del trattamento dei dati, rappresentate nel caso di specie dal bisogno di contrastare il terrorismo e la criminalità internazionale, e la conservazione dei dati per un periodo massimo di cinque anni dopo la partenza dei passeggeri dal Canada, senza che sia richiesto un collegamento con le finalità di contrasto al terrorismo internazionale, eccede i limiti di quanto strettamente necessario. Alla pari, eccede il limite della necessità anche il fatto che l'autorità canadese responsabile del trattamento dei dati possa comunicarli ad altre autorità nazionali, anche appartenenti a Paesi terzi[288]. Altri due aspetti problematici riguardano, infine, la mancanza di un adeguato sistema di notifica al soggetto i cui dati vengono raccolti e di un organismo indipendente a garanzia della tutela dei diritti[289].

In conclusione, questa pronuncia sembra allinearsi con il recente orientamento giurisprudenziale espresso dalla Corte di giustizia in materia di tutela dei dati personali, in cui è chiamata a bilanciare da un lato il bisogno di tutela il diritto alla privacy e dei dati personali e, dall'altro lato, la necessità di tutelare la sicurezza nazionale, attribuisce maggiore peso al primo elemento rispetto al secondo "purtuttavia senza mettere totalmente da parte queste ultime, anzi valorizzandole in un quadro di mantenimento delle garanzie democratiche"[290].

3.1.1 La dottrina del margine di apprezzamento

La dottrina del margine di apprezzamento, tradizionalmente utilizzata nella giurisprudenza della Corte europea dei diritti umani, vede in realtà una discreta applicazione anche da parte dei giudici di Lussemburgo. Invero, inizialmente utilizzata in materia di sicurezza ed ordine pubblico e nella politica della pesca ed agricoltura[291], è stata poi estesa anche all'ambito della tutela dei diritti fondamentali e, in particolare, con riferimento alla libertà

[288]Per un'analisi dettagliata degli aspetti critici dell'accordo cfr. anche B. SIEMEN, *The EU-US Agreement on Passenger Name Records and EC-Law: Data Protection Competences and Human Rights Issues in International Agreement of the Community*, in *German Yearbook of International Law* 2015, pag. 629.
[289]Cfr. C. GRAZIANI, *PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE on line* 2017, pag. 963.
[290]*Ibidem*, pag. 964.
[291]Utilizzando quale criterio di ricerca sul sito della Corte di giustizia www.curia.it le parole chiave "margin of discretion" appaiono quasi tremila risultati.

di espressione e al rispetto della vita privata e familiare. Il margine di apprezzamento, che nel sistema europeo viene spesso chiamato anche "margine di discrezionalità", svolge ivi diverse funzioni, tra cui quella, alla pari di quanto previsto nella giurisprudenza CEDU, di risolvere i conflitti in cui sono in gioco una libertà comunitaria e un diritto fondamentale dell'individuo.

Uno dei casi più esemplificativi al riguardo è la sentenza *Frede Damgaard*[292], avente ad oggetto la condanna di un cittadino danese da parte delle autorità giudiziarie nazionali per avere pubblicato sul proprio sito delle informazioni relative alle proprietà benefiche di un medicinale, la cui vendita e distribuzione era stata però vietata nel paese. La Corte di giustizia, chiamata a pronunciarsi quindi sul rapporto fra libertà di espressione e la tutela della salute pubblica, affermava che "È pacifico che il margine di valutazione discrezionale di cui dispongono le autorità competenti per stabilire dove si trovi il giusto equilibrio tra la libertà di espressione e gli obiettivi sopra menzionati è variabile per ciascuno degli scopi che giustificano la limitazione di tale diritto e secondo la natura delle attività considerate […]"[293]. In questo caso, inoltre, è esplicito il richiamo operato all'articolo 10 CEDU, e ai criteri indicati sia al secondo comma della norma in esame, sia dalla giurisprudenza della Corte di Strasburgo, per far sì che le misure limitative al diritto alla libertà di espressione possano dirsi conformi al sistema di tutela dei diritti umani[294].

E' interessante notare, infine, che "mentre nel sistema CEDU il margine di apprezzamento viene utilizzato per legittimare deroghe alla tutela dei diritti fondamentali, in quello comunitario esso amplia la tutela degli stessi. La Corte di giustizia, infatti, consente allo Stato di accordare la tutela più ampia ai diritti fondamentali così come concepiti del proprio ordinamento, anche ove questo si realizzi a detrimento di una libertà comunitaria"[295].

[292]Corte di giustizia, *Frede Damgaard*, sentenza del 2 aprile 2009, C-421/2007.
[293]*Ibidem,* par. 27.
[294]*Ibidem*, par. 26.
[295]I. ANRÒ, *Il margine di apprezzamento nella giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei Diritti dell'Uomo,* in *La funzione giurisdizionale nell'ordinamento internazionale e nell'ordinamento comunitario: atti dell'Incontro di studio tra i giovani cultori delle materie internazionalistiche, 7. edizione, Torino 9-10 ottobre 2009* (a cura di) A. ODENNINO, E. RUOZZI, A. VITERBO, F. COSTAMAGNA, L. MOLA, L. POLI, Napoli 2010, pagg. 21 e 22.

3.2 L'APPROCCIO DELLA CORTE EUROPEA DEI DIRITTI UMANI

I primi casi portati di fronte alla Corte europea dei diritti umani sul tema risalgono alla metà degli anni '80. In particolare, nella nota sentenza *Klass e altri c. Germania*[296], relativa a misure di intercettazione delle comunicazioni telefoniche e controllo della corrispondenza da parte delle autorità tedesche, i giudici di Strasburgo hanno dovuto affrontare per la prima volta il problema della "sorveglianza di massa", constatando come le suddette misure potessero costituire una minaccia per il diritto alla vita privata e familiare.

La Corte europea dei diritti umani infatti, pur riconoscendo agli Stati un certo margine di apprezzamento[297] nel decidere quali misure adottare al fine di garantire la sicurezza nazionale, ha ritenuto che l'articolo 8, comma 2, CEDU dovesse essere interpretato in maniera restrittiva e che, in ogni caso, le autorità nazionali dovessero prevedere delle garanzie effettive ed adeguate contro ogni possibile abuso[298], rinforzando, in particolare, il controllo giurisdizionale. Ad analoga conclusione i giudici di Strasburgo sono poi giunti nei successivi casi *Malone c. Regno Unito*[299] e *Kennedy c. Regno Unito*[300].

La Corte ritiene inoltre di fondamentale importanza, al fine di valutare la conformità della legislazione statale in materia di sorveglianza di massa con l'articolo 8 CEDU, verificare l'esistenza di rimedi effettivi in capo all'individuo. In questo contesto, infatti, se da un lato l'articolo 8 CEDU riveste un ruolo fondamentale dal punto di vista del diritto sostanziale, dall'altro lato deve essere anche tenuto in considerazione il diritto ad un ricorso effettivo di cui all'articolo 13 CEDU[301]. Sul punto, l'*ex* Presidente della Corte europea, Luzius Wildhaber affermava infatti che: "The Convention is all about remedies. In a sense, the existence of effective remedies is more important than the wording of the

[296]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, cit.
[297]Cfr. Y. ARAI-TAKANASHI, *op. cit.*, v. sopra nota 207, pag. 62.
[298]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, 6 settembre 1978, ricorso n. 5029/1971.
[299]Corte europea dei diritti umani, *Malone c. Regno Unito,* cit.
[300]Corte europea dei diritti umani, *Kennedy c. Regno Unito*, 18 maggio 2010, ricorso n. 26839/05.
[301]Nel caso *Rotaru c. Romania*, 4 maggio 2000, ricorso n. 28341/95, la Corte europea dei diritti umani aveva affermato che la specifica funzione dell'articolo 13 CEDU fosse quella di assicurare "availability at national level of a remedy to enforce the substance of the Convention rights and freedoms". Occorre però sul punto sottolineare come in realtà la Corte di Strasburgo non abbia sempre tenuto pienamente in considerazione l'articolo 13 CEDU in tema di misure di sorveglianza di massa. Ad esempio, nel caso Kennedy non era stata rinvenuta alcuna violazione dell'articolo 13, nonostante mancasse nell'ordinamento interno la previsione di una qualche forma di notifica successiva, e la Corte si era limitata a valutare la conformità della legislazione statale solo con riferimento agli articoli 6 e 8 CEDU.

Convention itself"[302].

Un concetto ricorrente nella giurisprudenza della Corte europea dei diritti umani è quello di "sorveglianza segreta", che viene definita come l'insieme di tutte le "misure di sorveglianza la cui esistenza rimane sconosciuta alle persone soggette al controllo"[303]. È il caso, per esempio, delle intercettazioni delle comunicazioni. Con il termine "collezione dei dati" ci si riferisce, invece, alla collezione e alla conservazione dei dati da parte dei servizi di intelligence, senza necessità che queste operazioni siano necessariamente condotte in segreto e riguardino conversazioni segrete[304]. "Naturally, secret data collection is a form of secret surveillance, but using both terms is useful to preserve some nuance in the discussion of the case-law if the European Court of Human Rights"[305]. Nei casi portati di fronte alla Corte europea dei diritti umani, si opera una distinzione fra "individual surveillance" – o, altrimenti detta, "targeted surveillance" - e "general programmes of surveillance" – altrimenti detta, "strategic monitoring"[306]. La maggior parte dei casi decisi dai giudici di Strasburgo a partire da *Klass e altri c. Germania* hanno riguardato misure di sorveglianza individuale. Le uniche pronunce finora decise relative alla "strategic monitoring" sono state *Weber e Saravia c. Germania*[307], *Liberty e altri c. Regno Unito*[308]e, più recentemente, *Roman Zakharov c. Russia* e *Big Brother Watch c. Regno Unito*[309].

In generale, si rileva un incremento dei ricorsi di fronte alla Corte europea solo negli ultimi anni. Infatti, se raffrontati ad altri diritti tutelati dalla CEDU, sono poche le sentenze rese negli ultimi trent'anni che hanno affrontato il problema della violazione dell'articolo 8, inizialmente sotto il profilo della tutela della vita privata, corrispondenza, e poi, successivamente, dei dati personali. Mette conto di osservare che il crescente interesse

[302]Disponibile alla pagina: http: //www.echr.coe.int/NR/rdonlyres/82597AB6-124F-48D5-8BBB-792899EB0C6A/0/AmeliorationsRecours_EN.pdf.
[303]Vedi Corte europea dei diritti umani (Corte Plenaria), *Klass e altri c. Germania*, par. 36.
[304]Per esempio, l'"Open-source intelligence" (OSINT) è un'attività di intelligence che ricava i dati da informazioni pubbliche come i social media, i giornali e le riviste accademiche. I servizi segreti raccolgono informazioni dai dati raccolti da entità pubbliche e private, quali le compagnie di telecomunicazioni, le istituzioni finanziarie.
[305]INSTITUTION FOR INFORMATION LAW (IViR) Document "TEN STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES", Amsterdam 2015, pag. 6.
[306]La distinzione fra i due tipi di raccolta di informazioni non risulta di così facile individuazione nei casi di sorveglianza di massa. Cfr. a riguardo Report FRA (European Union Agency for Fundamental Rights), *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update.* Disponibile alla pagina: http://fra.europa.eu/en/publication/2017/surveillance-intelligence-socio-lega
[307]Corte europea dei diritti umani, *Weber e Saravia c.* Germania, 29 giugno 2006, ricorso n. 54934/00.
[308]Corte europea dei diritti umani*, Liberty e altri c. Regno Unito*, 1 luglio 2008, ricorso n. 58243/00.
[309]Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito*, ricorso n. 58170/13.

sembra giustificarsi principalmente in ragione di una maggiore consapevolezza da parte degli individui del proprio diritto alla riservatezza e alla possibilità, resa evidente solo in seguito alle rivelazioni di Snowden, che le autorità statali possano adottare delle misure intrusive del suddetto diritto. Conseguentemente, gli individui hanno iniziato a far valere le proprie pretese sia di fronte a giudici nazionali sia di fronte ai tribunali internazionali e parallelamente è iniziato, soprattutto a livello normativo europeo, un processo di modificazione e adattamento - non ancora concluso - finalizzato ad una maggiore tutela dei propri dati personali.

È infatti ormai pacifico nelle pronunce della Corte europea dei diritti umani che l'adozione di misure di sorveglianza di massa e la collezione dei dati personali, ma anche la mera esistenza di misure legislative che autorizzano le suddette misure, possa costituire un'interferenza con l'articolo 8 della CEDU. Inoltre, così statuendo, i dati personali vengono fatti rientrare in via interpretativa nell'ampio concetto di diritto alla privacy[310].

3.2.1 La dottrina del margine di apprezzamento

Nel ragionamento dei giudici di Strasburgo in materia di tutela dei dati personali e delle limitazioni al diritto ai sensi dell'articolo 8, comma 2, CEDU, svolgono un ruolo fondamentale la dottrina del margine di apprezzamento e il principio del consenso.

Per quanto riguarda innanzitutto il margine di apprezzamento, inizialmente non vi era alcun espresso riferimento ad esso né nelle disposizioni normative della CEDU, né aveva costituito oggetto di discussione durante i lavori preparatori[311]. Esso costituisce pertanto il frutto di una lunga ed articolata evoluzione posta in essere sia a livello giurisprudenziale dalla Corte europea dei diritti umani sia a livello strettamente dottrinale[312]. La dottrina del margine di apprezzamento, di derivazione francese e

[310]Corte europea dei diritti umani, *Leander c. Svezia*, cit., par. 48 :"[…] Both the storing and the release of such information, which were coupled with a refusal to allow Mr. Leander an opportunity to refute it, amounted to an interference with his right to respect for private life as guaranteed by Article 8 § 1 (art. 8-1)". Cfr. anche Corte europea dei diritti umani, *Rotaru c. Romania*, cit., par. 43.

[311]Cfr. C. VAN DE HEYNING, *No place like home, Discretionary space for the domestic protection of fundamental rights*, in *Human Rights Protection in the European Legal Order: the interaction between the European and the National Courts*, edited by P. POPELIER, C. VAN DE HEYNING, P. VAN NUFFEL, Intersentia, 2011, pag. 83.

[312]Cfr. P. MAHONEY, F. MATCHER, H. PETZOLD, L. WILDHABER, *op. cit.,*v. sopra nota 204, pag. 147 e ss.

tedesca[313], era utilizzata inizialmente solo con riferimento all'articolo 15 CEDU e alla possibilità riconosciuta in capo agli Stati membri di invocare la deroga in caso di emergenza nazionale. In particolare, nel caso *Linguistico Belga*[314] del 1968 la Corte affermava che la CEDU implicava "[…] a just balance between the protection of the general interest of the Community and the respect due to fundamental human rights while attaching particular importance to the latter"[315]. Detto concetto è stato poi esteso, nel corso dei successivi anni, prima alla tutela della libertà di espressione sancita dall'articolo 10 CEDU - grazie soprattutto al caso *Handyside*[316] - poi al diritto di proprietà previsto nel Protocollo n. 1 e, infine, anche ad altri diritti tutelati dalla CEDU[317]. Ad oggi, si può affermare che la dottrina del margine di apprezzamento venga utilizzata soprattutto con riferimento agli articoli 8, 9, 10, 11 CEDU – riguardanti, rispettivamente, la tutela della vita privata e familiare, la libertà di espressione, la libertà religiosa e la libertà di riunione e di associazione. Per contro, alcun margine di discrezionalità è stato riconosciuto agli Stati con riferimento al diritto alla vita (articolo 2 CEDU) e al divieto di tortura e trattamenti inumani e degradanti (articolo 3 CEDU).

Occorre inoltre constatare che nel 2015 il margine di apprezzamento è passato dall'essere un principio di derivazione unicamente giurisprudenziale a venire espressamente inserito, grazie al Protocollo n. 15, nel preambolo alla Convenzione[318].
Per quanto riguarda il suo campo di applicazione, esso entra in gioco tutte le volte in cui la Corte europea dei diritti umani è chiamata a giudicare in merito ad una restrizione operata da parte di uno Stato al fine di perseguire uno scopo legittimo, quale può essere, ad esempio, la tutela della sicurezza nazionale. Agli Stati viene, infatti, lasciato un certo

[313]Utilizzato soprattutto nella giurisprudenza amministrativa. Cfr. in dottrina I. ANRÒ, *op. cit.*, vedi sopra nota 295.
[314]Corte europea dei diritti umani, *Caso Linguistico Belga (I)*, sentenza del 23 luglio 1968, ricorsi nn. 1474/62 e altri.
[315]*Ibidem*, par. 5.
[316]Corte europea dei diritti umani, *Handyside c. Regno Unito*, sentenza del 7 dicembre 1976, ricorso n. 5493/72. In questo caso si trattava di bilanciare l'articolo 10 CEDU, che sanciva il diritto alla libertà di espressione, e le esigenze di tutelare la morale. In particolare, ivi la Corte europea dei diritti umani affermava che «[…] Grâce à leurs contacts directs et constants avec les forces vives de leur pays, les autorités de l'Etat se trouvent en principe mieux placées que le juge international pour se prononcer sur le contenu précis de ces exigences comme sur la "nécessité" d'une "restriction" ou "sanction" destinée à y répondre(par. 48) ».
[317]Con riferimento, ad esempio, all'articolo 6 CEDU cfr. i casi Corte europea dei diritti umani, *Tolstoy Miloslavsky c. Regno Unito*, sentenza del 13 luglio 1995, ricorso n. 18139/91 e Corte europea dei diritti umani, *Kamasinski c. Austria*, sentenza del 19 dicembre 1989, ricorso n. 9783/1982.
[318]Nel preambolo si legge infatti: "che spetta in primo luogo alle Alte Parti contraenti, conformemente al principio di sussidiarietà, garantire il rispetto dei diritti e delle libertà definiti nella presente Convenzione e nei suoi protocolli e che, nel fare ciò, esse godono di un margine di apprezzamento, sotto il controllo della Corte europea dei Diritti dell'uomo istituita dalla presente Convenzione".

margine di discrezionalità nella scelta di quali misure adottare per raggiungere il suddetto scopo – come viene definita da alcuni una "forme atténuée d'immunité*"* dall'esercizio pieno della giurisdizione da parte della Corte europea dei diritti umani[319]. Questa scelta si giustifica in ragione della mancanza in seno agli Stati membri firmatari della CEDU di una concezione univoca dei diritti tutelati, essendo questi il frutto di un processo storico-politico e morale all'interno di una determinata società[320]. Il margine di apprezzamento non è però assoluto, bensì soggetto alla supervisione dei giudici di Strasburgo, che lo valutano non solo in relazione alla natura della restrizione ma anche alla natura del diritto coinvolto. Al fine di comprendere appieno la dottrina del margine di apprezzamento occorre, inoltre, considerare che la CEDU è uno "strumento vivente", che dev'essere quindi interpretata alla luce delle condizioni del momento[321].

La dottrina del margine di apprezzamento serve infatti a bilanciare, da un lato le esigenze di sovranità degli Stati – si ricordi, infatti, che l'esercizio della funzione giurisdizionale della Corte è fondato sul principio di sussidiarietà[322] - e, dall'altro lato, gli obblighi che questi Stati hanno nei confronti della CEDU. A tale riguardo, il giudice Martens nell'opinione dissenziente relativa al caso *Cossey c. Regno Unito* aveva specificato che:

" […] Dire que la Cour va réserver une marge d'appréciation aux États est une autre façon de dire que, consciente que sa position de juridiction internationale appelée à développer le droit dans un domaine sensible nécessite une certaine prudence, elle n'exercera pas à plein son pouvoir de vérifier si les États ont observé leurs engagements au titre de la Convention, mais ne constatera de violations que si l'on ne peut raisonnablement douter que les actes ou omissions des États en cause soient incompatibles avec ces engagements […] [323]".

[319]Cfr. P. MAHONEY, F. MATCHER, H. PETZOLD, L. WILDHABER, *op. cit.,*v. sopra nota 204, pag. 149.
[320]Cfr. F. PATRONI GRIFFI, *The margin of appreciation in the European Court's case-law*, in *Rivista Italiana di Diritto Comunitario* 2015.
[321]Cfr. E. BENVENISTI, *Margin of appreciation, consensus and universal standards*, in *International Law and Politics*, 1999, pag. 843.
[322]Cfr. J. CHRISTOFFERSEN, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*, Martenus Nijhoff Publishers, 2009, Olanda, pagg. 227 e ss. Sempre in dottrina cfr. anche S. DOTHAN, *Margin of Appreciation and Democracy: Human Rights and Deference to Political Bodies*, in *Journal of International Dispute Settlement* 2018, pagg. 145-153; A. LEGG, *The Margin of Appreciation in International Human Rights Law:Deference and Proportionality*, in *Human Rights Law Review* 2013, pagg. 795-797; J. KRATOCHVIL, *The Inflation of the Margin of Appreciation by the European Court of Human Rights*, in *Netherlands Quarterly of Human Rights* 2011, pagg. 324-357;.
[323]Corte europea dei diritti umani, *Cossey c. Regno Unito*, sentenza del 27 settembre 1990, ricorso n. 10843/84, Opinione dissenziente Giudice Martens, par. 3.6.3.

Nel corso degli ultimi anni, la dottrina del margine di apprezzamento è diventata uno strumento fondamentale utilizzato dalla Corte europea dei diritti umani al fine di decidere su temi molto sensibili come la libertà religiosa, la libertà di espressione e la protezione dei dati personali, giungendo spesso a soluzioni molto contrastanti rispetto a quelle rese, per esempio, solo qualche anno prima. Le ragioni di questi diversi approcci sono facilmente intuibili, se si considera che il margine di apprezzamento non ha regole codificate e la sensibilità dei giudici di Strasburgo è influenzata dal particolare momento storico in cui è chiamata a decidere[324]. Occorre inoltre ricordare che non tutti i diritti sanciti dalla CEDU sono assoluti, ma alcuni di essi, tra cui appunto gli articoli 8, 9, 10, possono essere soggetti, a determinate condizioni sancite dalle norme stesse, a delle limitazioni da parte degli Stati. In generale, si può affermare che nel contesto della lotta al terrorismo internazionale il margine di manovra lasciato agli Stati è molto ampio, dal momento che alcuni concetti come "altro pericolo pubblico che minacci la vita della nazione" di cui all'articolo 15, e "il rispetto della propria vita privata e familiare", ai sensi dell'articolo 8, sono tuttora difficili da definire e il loro contenuto può variare da un sistema nazionale all'altro[325]. Un ruolo fondamentale è ivi svolto dal requisito della prevedibilità: le autorità nazionali devono, infatti, adottare misure legislative idonee a garantire "adeguate ed effettive garanzie contro ogni abuso" e, in secondo luogo, devono garantire l'esistenza di organi giurisdizionali imparziali e trasparenti con il compito di sorvegliare e giudicare l'operato degli organi amministrativi che hanno adottato le misure di sorveglianza.

Strettamente connesso alla dottrina del margine di apprezzamento è il concetto di consenso. Anzi, più specificatamente, il margine di apprezzamento è inversamente proporzionale al consenso: la Corte europea dei diritti umani può infatti imporre un certo livello di protezione dei diritti fondamentali degli individui, riconoscendo quindi un ristretto margine di discrezionalità, sono nella misura in cui questo livello di protezione è garantito da un numero ampio di Stati. Con il termine consenso si indica, infatti "la ricerca effettuata dalla Corte di Strasburgo circa la sussistenza o meno di una concezione comune all'interno delle leggi e delle prassi degli Stati membri del Consiglio d'Europa"[326].

---

[324]Cfr. F. PATRONI GRIFFI, *op. cit.*, v. sopra nota 320, pag. 15 e ss.
[325]INSTITUTION FOR INFORMATION LAW (IViR) Document "TEN STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES", Amsterdam 2015, pag. 12.
[326]I. ANRÒ, *op. cit.*, v. sopra nota 295, pag. 12. Cfr. anche D. MCGOLDRICK, A *defence of the margin of Appreciation and an argument for its application by the Human Rights Committee*, in *International and Comparative Law Quarterly* 2016, pagg. 21-60.

Occorre inoltre sottolineare come l'ampio margine di apprezzamento lasciato agli Stati nel decidere quali misure adottare al fine di perseguire gli scopi legittimi di sicurezza nazionale, non implichi, però, che gli Stati possano liberamente interpretare gli obblighi internazionali derivanti dall'articolo 8 CEDU *à la carte*. La Corte europea dei diritti umani ha, infatti, costantemente affermato che, innanzitutto, il margine di apprezzamento non è illimitato bensì soggetto al rigido controllo giurisdizionale e che, in secondo luogo, malgrado il suddetto margine, gli stati devono rispettare degli standard minimi di tutela, imposti dalla Corte stessa, affinché la normativa nazionale possa dirsi conforme all'articolo 8 CEDU.

È interessante constatare come la dottrina del margine di apprezzamento sia stata utilizzata in questo contesto anche la Corte di giustizia nel caso *Digital Rights Ireland Ltd*, analizzato nei paragrafi precedenti del presente capitolo, al fine di valutare la compatibilità della direttiva europea 2006/24/CE in materia di comunicazioni elettroniche con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In particolare la Corte di giustizia, richiamando le considerazioni svolte dai giudici di Strasburgo nel caso *S. e Marper c. Regno Unito*[327], ha ritenuto che il potere discrezionale del legislatore europeo non fosse da considerarsi illimitato e andasse pertanto valutato con riferimento al "settore interessato, la natura dei diritti di cui trattasi garantito dalla Carta, la natura e la gravità dell'ingerenza nonché le finalità di quest'ultima"[328]. Sulla base di questi criteri, e in ragione del fatto che la normativa europea in esame permetteva la raccolta indiscriminata e generalizzata dei dati personali, senza alcuna distinzione né limitazione, era stato ritenuto che la stessa non tutelasse sufficientemente i dati personali degli individui.
Il suddetto richiamo alla giurisprudenza CEDU costituisce un ulteriore segnale della reciproca influenza tra i due organi giurisdizionali europei in materia di sorveglianza di massa e del bisogno di protezione dei diritti fondamentali delle persone.

[327]Corte europea dei diritti umani (GC), *S. e Marper c. Regno Unito,* cit., par. 87.
[328]Corte di giustizia (Grande Sezione), *Digital Rights Irlanda Ltd,* cit., par. 47.

3.2.2 Il principio di proporzionalità

Il principio di proporzionalità, strettamente connesso alla dottrina del margine di apprezzamento esposta nel paragrafo precedente, deriva dal diritto costituzionale e amministrativo tedesco[329] e può essere generalmente suddiviso in tre indipendenti, interconnessi, sotto-principi: il principio di adeguatezza, il principio di necessità e, infine, il principio di proporzionalità in senso stretto[330].

Tradizionalmente, "[…] the principle of proportionality rests on the assumption that States must act rationally; State must act in pursuit of some administrative or political objective, and they must apply suitable and proportionate measures. The focus on rationality is not foreign to law as legal theory has emphasized the importance of aims in law at least since the late 19th Century"[331].

Per quanto riguarda, nello specifico, il sistema di tutela previsto dalla CEDU, la Corte europea dei diritti umani non ha mai pienamente applicato e recepito il principio di proporzionalità – non potendo in realtà fare diversamente dato il suo ruolo di organo giurisdizionale sussidiario e non avendo, quindi, le stesse le competenze attribuite né ai giudici nazionali, né alla Corte di giustizia dell'Unione europea. Quest'ultima, infatti, avendo tra le varie funzioni anche quella di vigilare sul rispetto dei trattati[332], può applicare il giudizio di proporzionalità in maniera più rigorosa.

Orbene, la mancanza da parte dei giudici di Strasburgo di una chiara ed univoca applicazione del suddetto principio, ha spesso interferito sulla prevedibilità e la certezza dell'intero sistema CEDU. Invero, nonostante sia ormai pacifico il suo utilizzo nel giudizio

---

[329]Per un'analisi più approfondita del principio di proporzionalità del diritto costituzionale ed amministrativo cfr. M. POTO, *The Principle of Proportionality in Comparative Perspective*, in *German Law Journal* 2007, pagg. 835-870; R. SINGER, *Proportionate Thoughts About Proportionality,* in *Ohio State Journal of Criminal Law,* 2010, pagg. 218-250. Secondo alcuni autori le origini del principio di proporzionalità sono in realtà molto più datate, potendosi ritenere lo stesso alla base della legge del taglione di Hammurabi. A riguardo cfr. A. RISTROPH, *Proportionality as a Principle of Limited Government*, in *Duke Law Journal* 2005, pagg. 263-331.

[330]Cfr. N. EMILIOU, *The Principle of* Proportionality in European Law: a comparative study, Kluwer Law International, 1996, pagg 24-16.

[331]J. CHRISTOFFERSEN, *op. cit.*, v. sopra nota 322, pag. 166. Cfr. anche I. BUFFARD, K. ZEMANEK, *The "Object and Purpose" of a Treaty: an Enigma?,* in *Austrian Review of International EE European Law*, 1998, pagg. 311-343.

[332]Articolo 17 TUE "1.La Commissione promuove l'interesse generale dell'Unione e adotta le iniziative appropriate a tal fine. Vigila sull'applicazione dei trattati e delle misure adottate dalle istituzioni in virtù dei trattati. Vigila sull'applicazione del diritto dell'Unione sotto il controllo della Corte di giustizia dell'Unione europea. Dà esecuzione al bilancio e gestisce i programmi. Esercita funzioni di coordinamento, di esecuzione e di gestione, alle condizioni stabilite dai trattati. Assicura la rappresentanza esterna dell'Unione, fatta eccezione per la politica estera e di sicurezza comune e per gli altri casi previsti dai trattati. Avvia il processo di programmazione annuale e pluriennale dell'Unione per giungere ad accordi interistituzionali".

di valutazione in merito alle limitazioni agli articoli 8-11 CEDU[333], la Corte europea dei diritti umani non ha mai fornito dettagliate indicazioni in merito logica sottostante il suddetto giudizio[334].

In generale, nelle sentenze della Corte di Strasburgo il principio di proporzionalità svolge una duplice funzione, ossia di bilanciare due contrapposti interessi in gioco – rappresentati, quasi sempre, da un lato dal bisogno di tutelare i diritti del singolo e, dall'altro lato, dal perseguimento di finalità di tipo pubblicistico da parte degli organi statali - e di valutare la ragionevolezza e l'adeguatezza delle misure adottate rispetto al fine perseguito[335].

In relazione al giudizio di proporzionalità possono, generalmente, identificarsi quattro dottrine. La prima è il già citato test della rilevanza e della sufficienza - per la cui descrizione si rimanda al capitolo precedente[336] – che serve a valutare principalmente la sussistenza del requisito dello scopo legittimo.

La seconda è, invece, la cosiddetta "less restrictive alternative dottrine", con cui i giudici di Strasburgo verificano se gli Stati avrebbero potuto adottare, per raggiungere gli stessi obiettivi, misure meno intrusive del diritto tutelato. "The Court empirically and factually assesses the various alternatives, then chooses one of the most effective and less burdensome on the interference of the individual rights after a strict balance between the advantages and disadvantages"[337]. In questo tipo di valutazione assume un peso importante il principio di proporzionalità e sugli Stati incombe, inoltre, l'onere di dimostrare l'effettiva necessità delle suddette misure[338].

Infine, grazie alla dottrina del metodo comparativo e dell'interpretazione evolutiva, vengono risolti i problemi interpretativi connessi all'articolo 8 CEDU tenendo conto, da un lato, dell'evoluzione sociale e il particolare momento storico in cui si è chiamati a decidere sulla controversia e, dall'altro lato, delle origini e delle finalità iniziali dei redattori della Convenzione attraverso i *travaux préparatoires.* Purtroppo però, occorre sottolinearlo, i

[333]Cfr. P. DE SENA, *Proportionality and human rights in international law: some…"utilitarian" reflections*, in *Rivista di diritto internazionale* 2016, pag. 1011.
[334]Cfr. F. JIZENG, *Rethinking the Method and Function of Proportionality Test in the European Court of Human Rights,* in *The Journal of Human Rights* 2016, pag. 51.
[335]*Ibidem*, pag. 46. In questo contesto, in particolare, il principio di proporzionalità non svolge la funzione di *riconciliare* due interessi (o principi) contrastanti, bensì di farne *prevalere* uno rispetto all'altro. Cfr. sul punto P. DE SENA, *op. cit.* v. sopra nota 333, pag. 1024.
[336]Cfr. paragrafo 2.2.1.1.
[337]Cfr. F. JIZENG, *op. cit.,* vedi sopra nota 334, pag. 83.
[338]Y. ARAI-TAKAHASHI*, op. cit.*, v. sopra nota 207, pag. 91.

lavori preparatori sono sempre risultati poco utili al fine di comprendere la portata applicativa del diritto alla privacy[339], soprattutto sotto il profilo della protezione dei dati personali che interessa il presente elaborato, data la totale mancanza di qualsiasi conoscenze tecnica a riguardo nel momento in cui la CEDU è stata redatta.

Pur non venendo esplicitamente richiamato dalla CEDU, il principio di proporzionalità è diventato uno dei parametri fondamentali utilizzato dalla Corte europea dei diritti umani per valutare la sussistenza di una violazione dell'articolo 8 CEDU. Ad esempio, già nella più risalente sentenza *Weber e Saravia c. Germania*, veniva ritenuto necessario valutare *in primis* se la misura fosse proporzionata ai fini perseguiti e, poi, solo in caso di risposta affermativa, si sarebbe passati al giudizio in merito al rispetto dei principi di legittimità e necessità[340].

Nel delicato contesto della raccolta dei dati personali e delle misure di sorveglianza di massa[341], la Corte europea dei diritti umani sembra applicare rigorosamente il suddetto principio, al fine di valutare la gravità della misura di interferenza con l'articolo 8 CEDU, dando quindi la priorità - nel giudizio di bilanciamento - ai potenziali effetti sui diritti degli individui, rispetto alla legittimità ed all'utilità del fine perseguito[342]. Conseguentemente, incombe sulle autorità nazionali l'onere di provare che le misure adottate siano necessarie e appropriate rispetto al fine perseguito, ossia che non sia stato possibile adottare misure meno intrusive dei diritti degli individui per il raggiungimento delle medesime finalità [343] .

Alla pari, la Corte di giustizia nel caso *Digital Rights Ireland Ltd* ha fondato sul principio di proporzionalità la valutazione in merito alla compatibilità della direttiva 2006/24/CE con i principi sanciti dagli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea[344]. Ivi è stato, infatti, constatato che la memorizzazione dei dati relativi al traffico di comunicazione e alla localizzazione permetteva di fatto di trarre delle conclusioni in merito ad aspetti rilevanti della vita degli individui ed eccedesse quindi i limiti di quanto strettamente necessario per il raggiungimento degli obiettivi fissati dal

[339]M.J. VELU, *op. cit.*, v. sopra nota 201, pag. 39. In particolare, l'articolo 8 CEDU trae origine dalla Raccomandazione n. 38 dell'Assemblea Consultativa, adottata l'8 settembre 1949.
[340]Corte europea dei diritti umani, *Weber e Saravia c. Germania,* cit., par. 107.
[341]Corte europea dei diritti umani, *Big Brother and Watch e altri c. Regno Unito*, cit., par. 384; Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria*, cit., par. 71; Corte europea dei diritti umani (GC), *Zakharov c. Russia*, cit., parr. 262 e 263.
[342]Y. ARAI-TAKAHASHI*, op. cit.*, v. sopra nota 207, pag. 74.
[343]F. JIZENG, *op. cit.*, v. sopra nota 334, pag. 46.
[344]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd,* cit., par. 69.

legislatore europeo. In ogni caso, per l'analisi relativa agli altri aspetti critici della sentenza in esame, si rimanda a quanto già precedentemente esposto nel paragrafo 3.1. del presente capitolo.

3.2.3 Lo *status* di vittima

Uno dei primi e più importanti aspetti problematici evidenziati nella giurisprudenza della Corte europea dei diritti umani in materia di protezione dei dati personali ha riguardato lo *status* di vittima e la corrispondente possibilità in capo agli individui di fare ricorso per violazione dell'articolo 8 CEDU.

Invero i giudici di Strasburgo hanno dimostrato negli ultimi anni una particolare sensibilità per le problematiche connesse alla sorveglianza di massa, rendendo di fatto possibile, a certe condizioni, il ricorso giurisdizionale in *abstracto*, in deroga a quanto previsto dall'articolo 34 CEDU. In base alla suddetta norma, un individuo può presentare ricorso solo qualora dimostri di essere vittima di una violazione di uno dei diritti riconosciuti dalla Convenzione da parte degli Stati contraenti. I ricorrenti non possono richiedere che venga condotto uno scrutinio in astratto sugli atti legislativi ed amministrativi adottati dalle autorità statali per presunta contrarietà ad un diritto sancito dalla CEDU. Non rientra infatti tra i compiti dei giudici di Strasburgo quello di valutare la legittimità delle scelte operate dai parlamenti nazionali – che resta prerogativa dei giudici interni in virtù del principio di sussidiarietà che regola l'operato della Corte europea dei diritti umani – ma essi devono limitarsi ad accertare l'ingiustizia subita dall'individuo per la violazione di un diritto umano sancito nella CEDU. Conseguentemente i ricorrenti, al fine di riuscire a far valere in questo contesto le proprie pretese in giudizio, devono dimostrare che le misure statali di interferenza li interessino direttamente. Per questo motivo, la Corte ha, tendenzialmente, sempre evitato di esaminare i ricorsi in astratto.

Le decisioni in materia di sorveglianza di massa e misure di intercettazione costituiscono pertanto un'eccezione significativa[345]. Dall'analisi complessiva della

[345]Questa impostazione è stata criticata dal giudice Dedov nella sua opinione concorrente relativa al caso *Roman Zakharov c. Russia*. Ivi, infatti, il giudice russo ha sollevato dei dubbi in merito alla correttezza della Corte europea dei diritti umani a giudicare, in mancanza di una procedura pilota, la legge nazionale. Inoltre, sempre secondo Dedov, tutte le violazioni della Convenzione riconosciute negli anni si sono fondate principalmente sull'abuso di poteri da parte delle pubbliche autorità. Ma essendo l'abuso una questione più legata all'etica che alla qualità normativa, il problema non può essere eliminato semplicemente dichiarando

giurisprudenza della Corte europea dei diritti umani in questa materia sono emersi due differenti approcci. Secondo un primo approccio, che si può definire più restrittivo, lo *status* di vittima non andrebbe interpretato in maniera così ampia da ricomprendere, potenzialmente, ogni individuo che teme che i servizi segreti nazionali possano raccogliere ed utilizzare le sue informazioni personali. Occorre, infatti, che sussista una ragionevole probabilità – "reasonable likehood" – che le autorità pubbliche stiano raccogliendo i dati personali proprio relativi a quell'individuo. Secondo un secondo approccio meno rigoroso, che risulta essere stato adottato più di recente dai giudici di Strasburgo in ragione delle riscontrate difficoltà per i ricorrenti di dimostrare che le misure di sorveglianza, in quanto appunto segrete, abbiano costituito un'illegittima interferenza nella vita privata e familiare, è possibile riconoscere a certe condizioni lo *status* di vittima sulla base della mera esistenza delle relative misure legislative nazionali.

Già nel precedentemente citato caso *Klass e altri c. Germania* era stato affermato che fosse sufficiente per il ricorrente dimostrare, al fine di vedersi riconosciuto il proprio *status* di vittima in astratto per violazione dell'articolo 8 CEDU, di trovarsi in una situazione di "[…] reasonable risk of his being subjected to secret surveillance"[346]. A tal fine, la Corte europea dei diritti umani doveva tenere in considerazione la natura dei diritti violati, il carattere segreto delle misure di sorveglianza e la potenziale connessione tra le stesse e i diritti dell'individuo[347]. Invero, con il termine "reasonable likelihood" si indicava la necessità che per il ricorrente sussistesse il concreto rischio di subire delle conseguenze negative in ragione delle misure di sorveglianza, soprattutto nella misura in cui queste informazioni venissero messe a disposizione delle autorità statali e raccolte tramite intercettazioni segrete[348].

Con la successiva pronuncia *Malone c. Regno Unito*[349], la Corte europea dei diritti umani aveva ulteriormente specificato i criteri e le condizioni necessarie per valutare il ricorso sulla base della mera esistenza di misure legislative di sorveglianza, al fine di

---

la legge contraria ai diritti umani. Cfr. Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, sentenza del 4 dicembre 2015, ricorso n. 47143/06, opinione concorrente del giudice Dedov, pag. 84.

[346]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, cit., par. 31.

[347]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania,* cit., par. 34. In maniera analoga si esprime la Corte europea dei diritti umani anche nei casi *Malone c. Regno Unito*, cit., par. 86; *Case of The Association For European Integration And Human Rights And Ekimdzhiev c. Bulgaria,* 28 giugno 2007, ricorso n. 62540/00, par. 58.

[348]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, sentenza del 4 dicembre 2015, ricorso n. 47143/06, opinione concorrente del giudice Dedov, pag. 87.

[349]Corte europea dei diritti umani (Plenaria), *Malone c. Regno Unito*, cit..

riconoscere o meno la violazione dell'articolo 8 CEDU. Inoltre, nel caso *Mersch e altri c. Lussemburgo*[350] la Commissione europea dei diritti umani aveva riconosciuto, tra gli elementi rilevanti per fare valere lo *status* di vittima in astratto, anche la mancanza nel sistema nazionale di un qualche obbligo di notifica, da effettuare anche *ex post*, nei confronti del soggetto destinatario delle interferenze.

Infine, nel più recente caso *Kennedy c. Regno Unito*, il test del "reasonable likehood" è stato ulteriormente elaborato, ricomprendendo quale parametro di valutazione la disponibilità di rimedi (giurisdizionali) a livello nazionale e il rischio che le misure di sorveglianza possano essere applicate nei confronti del ricorrente[351]. In questi casi, infatti, "[…] widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is a greater need for scrutiny by this Court"[352].
Nel contesto in esame, un ulteriore elemento tenuto costantemente in considerazione dai giudici di Strasburgo, soprattutto a partire dal caso *Iordachi c. Moldavia*[353], ha riguardato la particolare categoria o gruppo di persone cui apparteneva il ricorrente, che lo avrebbero reso potenzialmente più a rischio di altri di essere destinatario di misure di sorveglianza. Ad esempio, nella precitata sentenza era stato riconosciuto al signor Iordachi e agli altri ricorrenti lo *status* di vittima sulla base del fatto che essi, in qualità di avvocati difensori dei diritti umani e in continuo contatto con persone accusate di avere commesso dei reati, potevano ragionevolmente considerarsi destinatari di intercettazioni segrete da parte delle autorità statali[354].

In tempi più recenti, la Corte europea dei diritti umani è tornata ad occuparsi dei problemi connessi alla sorveglianza di massa e al ricorso in astratto nella sentenza resa dalla Grande Camera il 4 dicembre 2015 nel caso *Roman Zakharov* c. *Russia*[355]. Il caso in esame riguardava il caporedattore di una casa editrice e di un giornale di aviazione e capo della sezione di San Pietroburgo di una ONG che monitorava lo stato di libertà dei media

[350]Commissione europea dei diritti umani (Plenaria), *Mersch e altri c. Lussemburgo*, ricorsi nn. 10439/83 e altri, sentenza del 10 maggio 1985; cfr. anche Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania,* cit., par. 58.
[351]Corte europea dei diritti umani, *Kennedy c. Regno Unito*, cit., parr. 112, 123 e 126.
[352]*Ibidem*, par. 124.
[353]Corte europea dei diritti umani, *Iordachi c. Moldavia*, 10 febbraio 2009, ricorso n. 25198/02. In particolare, qui i giudici di Strasburgo hanno constatato la mancanza del requisito del "previsto dalla legge", sotto il profilo della prevedibilità.
[354]Corte europea dei diritti umani, *Iordachi c. Moldavia*, cit., parr. 31 e 34.
[355]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit.

nella regione, la libertà di espressione e il rispetto dei diritti dei giornalisti ed offriva loro anche supporto legale. Nel dicembre 2003 il Sig. *Zakharov* citava a giudizio tre operatori di rete mobile, sostenendo che vi fosse stata un'intrusione nella privacy delle sue comunicazioni telefoniche. Il controllo telefonico era stato reso possibile grazie ad un Decreto Ministeriale che permetteva ai servizi segreti russi di installare apparecchiature per intercettare tutte le comunicazioni senza previa autorizzazione giudiziaria. I tribunali nazionali rigettavano i ricorsi, sostenendo che non fosse stata fornita alcuna prova dell'effettiva esistenza dell'intercettazione e della relativa intrusione nella vita privata a familiare[356].

Questa pronuncia ha assunto un'importanza significativa nel contesto in esame, dal momento che ivi i giudici hanno ripercorso tutta la giurisprudenza recente in materia di sorveglianza segreta e misure di interferenza con il diritto alla privacy tutelato dall'articolo 8 CEDU, sviluppando e cristallizzando le due condizioni necessarie per fare valere il ricorso sulla base del "reasonable likehood", senza dovere ulteriormente dimostrare di essere in concreto destinatari di intercettazioni[357]. A tal fine, occorre in particolare avere riguardo all'ambito di applicazione della legge, verificando se l'individuo potrebbe esserne potenzialmente affetto e se, inoltre, egli abbia la possibilità di ricorrere a qualche rimedio giurisdizionale. In presenza di quest'ultima condizione risulta più difficile ritenere che le pubbliche autorità abbiano abusato dei propri poteri e incombe pertanto sul ricorrente l'onere di provare, al fine di riuscire a far riconoscere la violazione del diritto alla privacy sulla base della mera esistenza di misure di intercettazione, che, in ragione del sua particolare situazione, egli può essere considerato una potenziale vittima delle stesse[358].

In definitiva si può quindi affermare che, ogni qualvolta la questione portata dinnanzi alla Corte europea dei diritti umani riguardi delle misure di intercettazione delle comunicazioni e la loro potenziale interferenza con il diritto alla vita privata e familiare sancito dall'articolo 8 CEDU, la stessa debba verificare, innanzitutto, se i ricorrenti appartengano ad un particolare gruppo o categoria di persone potenzialmente a rischio di intercettazioni - come possono essere, ad esempio, coloro che svolgono attività di critica al

[356] Cfr. M. FRANCHI, I. VIARENGO, *Tutela Internazionale dei Diritti Umani*, *Casi e materiali,* Giappichelli, Torino 2016, pag 221.
[357] Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia,* cit., parr. 163-169.
[358] *Ibidem*, cit., par. 171.

governo o collaborano con ONG che lottano per la tutela della libertà di espressione o il diritto alla privacy.

In secondo luogo, poi, è necessario accertare l'esistenza, e soprattutto l'efficacia, dei rimedi giurisdizionali previsti a livello nazionale per tutelare gli individui da eventuali abusi da parte soprattutto delle autorità amministrative[359]. Infatti, nel caso in cui la legislazione nazionale non preveda i suddetti rimedi "[...]the menace of surveillance can be claimed in itself to restrict free communication through the postal and telecommunication services, thereby constituting for all users or potential users a direct interference with the right guaranteed by Article 8 […]"[360].

Per quanto riguarda nello specifico il caso *Zakharov c. Russia*, la Grande Camera ha rilevato sia l'insufficienza dei rimedi esperibili dai ricorrenti a livello giurisdizionale[361] sia l'uso massiccio ed indiscriminato delle misure di sorveglianza da parte dei servizi di *intelligence*, per cui ha ritenuto giustificato riconoscere lo *status* di vittima ai ricorrenti sulla base della mera esistenza della legislazione e, conseguentemente, analizzare la fattispecie in astratto"[362].

In particolare, i giudici di Strasburgo hanno ritenuto necessario valutare la natura delle offese, la categorie di persone potenzialmente a rischio di intercettazioni, l'accessibilità e la chiarezza della legge, le finalità e la durata delle misure di sorveglianza, le procedure da seguire per la raccolta, la memorizzazione, l'utilizzo e la distruzione dei dati, le procedure di autorizzazione e di controllo (giurisdizionale) e, infine, i meccanismi di notifica[363].

L'approccio adottato dalla Corte europea dei diritti umani nel caso *Roman Zakharov c. Russia* è stato poi confermato nel successivo caso *Szabo e Vissy c. Ungheria*[364], relativo ad un ricorso presentato da due membri di un'organizzazione no-profit che svolgeva attività di critica al governo. Nel 2011 il governo ungherese aveva infatti promulgato una legge antiterrorismo, con il quale era stata istituita una *task force* specializzata nella raccolta di informazioni confidenziali relative alla vita dei cittadini, con la possibilità di effettuare delle ricerche e adottare misure di sorveglianza sul domicilio, l'apertura della

[359]Sul punto cfr. anche M. PALMISANO, *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their application to mass surveillance in the United States and Russia*, in *Gonzaga Journal of International Law*, 2017, pagg. 85-87.
[360]Corte Europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., par. 171.
[361]*Ibidem*, par. 176.
[362]*Ibidem,* parr. 178 e 298.
[363]*Ibidem*, par. 238.
[364]Corte Europea dei diritti umani, *Szabo e Vissy c. Ungheria*, cit.

corrispondenza, monitoraggio e memorizzazione del contenuto di comunicazioni elettroniche o computerizzate. Le informazioni venivano collezionate senza il permesso dei destinatari e senza alcuna specifica autorizzazione da parte dell'autorità giudiziaria. Tutto questo veniva realizzato al fine di proteggere la sicurezza nazionale. Nel 2012 i due ricorrenti facevano ricorso alla Corte Costituzionale, ritenendo che la legge antiterrorismo violasse il loro diritto costituzionale alla privacy. La Corte Costituzionale accoglieva però soltanto la parte del ricorso relativa all'ordine autorizzativo del giudice, rigettando la domanda per la restante parte.

Il caso veniva quindi portato di fronte alla Corte europea dei diritti umani, la quale, richiamando il ragionamento espresso nella sentenza *Zakharov c. Russia,* non si riteneva persuasa del fatto che la legge ungherese alla sezione "7/E (3) sorveglianza" prevedesse sufficienti e adeguate garanzie contro eventuali abusi da parte delle pubbliche autorità[365]. Inoltre, le misure di sorveglianza potevano potenzialmente interessare tutti e venivano adottate dal potere esecutivo senza alcun controllo preventivo o successivo da parte dell'autorità giudiziaria. Per tutti questi motivi, veniva riconosciuta la violazione dell'articolo 8 CEDU.

Sempre in materia di sorveglianza delle comunicazioni, occorre segnalare inoltre una più recente sentenza emessa il 18 luglio 2017, *Mustafa Sezgin Tanrikulu c. Turchia*[366]. Il ricorrente, già membro del Parlamento turco e all'epoca dei fatti presidente dell'Associazione di avvocati Diyarbakir, lamentava di essere stato vittima di intercettazioni della telefonia e delle comunicazioni elettroniche poste in essere dall'Agenzia di Intelligence Turca (MIT).
In particolare, egli riteneva che il suo diritto alla privacy fosse stato violato dal fatto che le autorità nazionali turche, nell'adottare misure di sorveglianza al fine di prevenire atti di terrorismo, anche internazionale, identificare ed arrestare i possibili criminali, non avessero sufficientemente dimostrato che egli avesse effettivamente compiuto un fatto illecito sul territorio turco, o quanto meno ci fosse il ragionevole sospetto a riguardo. Infatti, anche in base a quanto stabilito dalla legge nazionale turca in materia, le intercettazioni erano possibili solo in presenza di un grave indizio di commessione di un reato – cosa che non era avvenuta nel caso di specie - e che, inoltre, fosse obbligatorio notificare l'avvenuta

[365]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria,* cit., par. 86.
[366]Corte europea dei diritti umani, *Sezgin Tanrikulu c. Turchia*, sentenza del 18 luglio 2017, ricorso n. 27473/06.

intercettazione alla persona interessata una volta terminata; per contro, egli aveva scoperto di essere destinatario delle misure solo indirettamente e tramite un articolo pubblicato sul giornale.
Al fine di decidere in merito alla violazione dell'articolo 8 CEDU, e alla possibilità di fare ricorso sulla base della mera esistenza di misure di intercettazione, la Corte europea dei diritti umani richiama nuovamente quanto già espresso in materia nel caso della Grande Camera *Roman Zakharov c. Russia.* In particolare essa rileva la mancanza, nel caso di specie, di qualsiasi rimedio successivo a favore della persona destinataria delle misure di intercettazione e, conseguentemente, riconosce alla stessa lo *status* di vittima in astratto ex articolo 34 CEDU.

Si rende infine opportuno analizzare due importanti sentenze rese dalla Corte europea dei diritti umani rispettivamente a giugno e settembre 2018. Entrambe hanno riguardato l'adozione di misure di sorveglianza di massa da parte delle autorità nazionali, rispettivamente in Svezia e nel Regno Unito. Nel primo caso *Centrum of Rattvisa c. Svezia*[367], il ricorso era stato presentato da una ONG che denunciava il rischio che la legge svedese sullo spionaggio potesse di fatto intercettare tutte le comunicazioni.
I giudici di Strasburgo hanno ivi nuovamente richiamato e applicato i criteri sanciti nel caso *Roman Zakharov c. Russia* – valutando, tra le altre cose, anche il ricorso in astratto e la possibilità di rimedi effettivi - e concluso che non vi era stata violazione dell'articolo 8 CEDU, dal momento che erano stati previsti a livello legislativo nazionale adeguati e sufficienti sistemi di garanzia contro eventuali abusi, quali l'autorizzazione preventiva[368] e diverse disposizioni che prevedevano l'obbligo di distruggere i dati raccolti[369]. Secondo la Corte, inoltre, anticipando quanto poi successivamente sviluppato nel caso *Big Brother Watch e altri c. Regno Unito*[370], la notifica successiva non era di per sé sempre obbligatoria, "[…] therefore, the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot by itself warrant the conclusion that the interference was not «necessary in a democratic society»,

[367]Corte europea dei diritti umani, *Centrum För Rättvisa c. Svezia*, cit.
[368]*Ibidem,* par. 141.
[369]*Ibidem*, parr. 145 e 181.
[370]Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito*, sentenza del 13 settembre 2018, ricorsi nn. 58170/13 e altri.

as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference"[371].

Degno di nota in questo contesto è inoltre il poc'anzi citato caso *Big Brother Watch e altri c. Regno Unito*, relativo ad un ricorso presentato da una ONG in seguito alle rivelazioni di Snowden che avevano reso noti i programmi di sorveglianza di massa posti in essere dai governi statunitense e inglese. Nella sentenza in esame, la Corte europea dei diritti umani sembra avere adottato un approccio "più cauto" nei confronti della sorveglianza di massa, precisando come essa non sia di per sé vietata e non debba essere necessariamente considerata come un abuso del margine di apprezzamento da parte degli Stati[372]. Invero, "[…] it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications"[373]. Ciononostante, è sempre necessario interpretare il margine di apprezzamento in maniera restrittiva, a causa della facilità con cui le misure di intercettazione possono essere in questo contesto soggette ad abusi[374].

Inoltre, in maniera continuativa con quanto già stabilito nel caso *Roman Zakharov c. Russia*[375], il requisito del controllo giurisdizionale viene sempre considerato come un "[…] important safeguard against arbitrariness […]"[376].

In conclusione, dalla sentenza appena esaminata sembrerebbe emergere un'impostazione della Corte europea dei diritti umani più incline a non ritenere di per sé illegittima la sorveglianza di massa, rappresentando essa in molti casi uno strumento efficace per perseguire le diverse finalità legittime indicate nell'articolo 8 CEDU – quali, ad esempio, la tutela della sicurezza nazionale sempre più minacciata dal fenomeno terroristico - ma a ricondurre la violazione del diritto alla privacy alla mancanza, a livello nazionale, di adeguati sitemi di controllo in capo ad organismi indipendenti[377].

---

[371] Corte europea dei diritti umani, *Centrum För Rättvisa c. Svezia,* cit., par. 164.
[372] Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito,* cit., par. 314.
[373] Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito,* cit., par. 316.
[374] *Ibidem*, par. 315.
[375] Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., 249.
[376] Corte europea dei diritti umani, *Big Brother Watch e altri c. Regno Unito,* cit., par. 318.
[377] *Ibidem*, par. 386.

3.2.4 Il controllo giurisdizionale e l'obbligo di notifica

La Corte europea dei diritti umani, inoltre, ben consapevole della portata e della pericolosità delle misure di sorveglianza di massa adottate dai governi, ha costantemente rilevato nella sua giurisprudenza[378] l'importanza e la necessità di rafforzare la trasparenza del potere giudiziario e di implementare l'utilizzo della successiva notifica in caso di violazione dei dati personali. Ad essa è infatti ricollegata l'effettiva possibilità per l'individuo di difendersi, in sede giurisdizionale contro eventuali abusi di potere posti in essere dagli organi incaricati di ordinare e dare esecuzione alle misure di intercettazione[379].

Invero, anche in base a quanto stabilito all'articolo 1 della Raccomandazione n. R (87) allegata alla Convenzione 108 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale – già analizzata nel paragrafo 5.2., del primo capitolo del presente elaborato – gli Stati membri devono dotarsi di un'autorità nazionale di controllo indipendente, che ha il compito di monitorare e denunciare eventuali violazioni della Convenzione. Al fine di stabilire il livello di indipendenza dell'organo di controllo, occorre avere riguardo alle funzioni da esso svolte, alle modalità con cui i membri vengono e all'esistenza di un sistema di norme che regoli il suddetto funzionamento[380].

In particolare, nel contesto della sorveglianza di massa deve essere garantita soprattutto l'indipendenza dal potere esecutivo[381]. Già nei casi *Klass* e *altri c. Germania* e *Weber e Saravia c. Germania,* la Corte europea dei diritti umani riteneva che sia i commissari G10 che i membri del Parlamento fossero sufficientemente indipendenti nell'esercizio delle proprie funzioni, per cui non veniva ravvisata alcuna violazione dell'articolo 8 CEDU[382]. Alla pari, gli organi giurisdizionali avrebbero dovuto preventivamente controllare ed autorizzare le misure di intercettazione disposte dal potere

[378]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, cit., par. 56 ; Corte europea dei diritti umani, *Kennedy c. Regno Unito*, cit., parr. 166 e 167.
[379]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit. par. 234.
[380]INSTITUTION FOR INFORMATION LAW (IViR) Document "TEN STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES", Amsterdam 2015, pag. 22.
[381]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, cit., par. 56.
[382]*Ibidem*, par. 56; Corte europea dei diritti umani, *Weber e Saravia c. Germania*, cit., parr. 55 e 113.

esecutivo. Al suddetto requisito era possibile, infatti, derogare solo in casi eccezionali e di comprovata urgenza[383].

Orbene, tornando al più recente caso della Grande Camera *Roman Zakharov c. Russia*, il requisito del controllo giurisdizionale sembrava essere soddisfatto solo con riferimento al controllo iniziale, mentre la successiva supervisione era affidata al Presidente, al Parlamento, al Governo, o al Procuratore Generale[384], organi quindi parziali. In realtà, a ben vedere, anche il controllo preliminare non era del detto immune da abusi, dal momento che le autorità russe potevano accedere direttamente ai dati delle comunicazioni senza bisogno di mostrare un'autorizzazione ai fornitori di servizi di comunicazione[385]. Alla pari, anche il National Security Act Ungherese non prevedeva alcun organo giurisdizionale autonomo ed indipendente con la funzione di autorizzare, monitore e revisionare le misure segrete di sorveglianza[386]. In base a quanto stabilito nella suddetta sentenza, infatti, in mancanza di un'autorizzazione giudiziaria *ex ante*, la normativa nazionale avrebbe dovuto garantire quanto meno un efficace ed effettivo sistema di controllo giurisdizionale *ex post*[387]. Orbene, nel caso ungherese sia il controllo preventivo sia quello successivo erano affidati ad un organo esecutivo dipendente e parziale, per cui nessuna adeguata tutela veniva garantita ai diritti dei singoli.

Una maggiore tutela del singolo tramite il meccanismo del controllo giurisdizionale è stata prevista, ad esempio, a livello legislazione europeo nell'articolo 28 della nuova direttiva (UE) 2016/680 relativa al trattamento e raccolta dei dati personali per finalità di indagine, accertamento di reati. Ivi è previsto infatti l'obbligo di consultazione preventiva all'autorità di controllo nazionale in due specifichi casi, ossia quando il trattamento presenti un elevato rischio per la tutela degli individui, senza che il titolare del trattamento abbia adottato a riguardo le adeguate misure[388], e quando il trattamento, in ragione dell'utilizzo di tecnologie, procedure o meccanismi nuovi, presenta un rischio elevato per i diritti e le libertà degli interessati[389].

---

[383]INSTITUTION FOR INFORMATION LAW (IViR) Document "TEN STANDARDS FOR OVERSIGHT AND TRANSPARENCY OF NATIONAL INTELLIGENCE SERVICES", Amsterdam 2015, pag. 16.
[384]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., par. 274.
[385]*Ibidem*, par. 270.
[386]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria*, cit., par. 75.
[387]M. D. COLE, A. VANDENDRIESSCHE, *op. cit.*, v. sopra nota 238, pag. 126.
[388]Articolo 28, par. 1 (a), direttiva (UE) 2016/680.
[389]Articolo 28, par. 1 (b), direttiva (UE) 2016/680.

Strettamente connesso al successivo controllo giurisdizionale è, inoltre, il meccanismo della notifica. Tramite esso, il soggetto può essere informato dell'esistenza di misure di intercettazione adottate nei suoi confronti e fare eventualmente ricorso ad un tribunale nazionale per vedere tutelate le proprie ragioni. Invero, in un contesto come quello della sorveglianza di massa in cui il rischio di abuso è molto alto[390], risulta fondamentale prevedere siffatte garanzie in capo agli individui al fine di garantire la tutela ricevuta ai sensi dell'articolo 8 CEDU[391]. In certi casi, però, la comunicazione al soggetto interessato dell'avvenuta raccolta dei suoi dati personali potrebbe, di fatto, annullare l'efficacia delle attività di *intelligence* o, nei casi più estremi, anche rivelare i nomi degli agenti che hanno svolto le suddette operazioni. Per questo motivo "[…] the fact that persons concerned by secret surveillance measures are not subsequently notified once surveillance has ceased cannot be itself warrant the conclusion that the interference was not "necessary in a democratic society", as it is the very absence of knowledge of surveillance which ensures the efficacy of the interference [..]"[392].

Inoltre, la Corte europea dei diritti umani ritiene che il bisogno di prevedere a livello legislativo nazionale la notifica successiva debba essere valutato in relazione alla singola fattispecie e che essa debba essere ritenuta necessaria solo qualora la pubblicità di alcune informazioni non dia luogo agli appena descritti rischi. Orbene, nel caso *Roman Zakharov* viene evidenziato come la mancanza di questo meccanismo di fatto annulli qualsiasi possibilità in capo ai individui di presentare ricorso o appello agli organi giurisdizionali competenti in caso di illegittime interferenze nella vita privata e familiare[393], comportando una violazione dell'articolo 8, par. 2, CEDU. Alla stessa conclusione giungono i giudici di Strasburgo nel caso successivo *Szabo e Vissy*[394]. Invero, il National Security Act, oltre a non prevedere alcun obbligo di notifica successiva in caso di abusi da parte di organismi statali, attribuisce la competenza a giudicare eventuali ricorsi al Ministro degli Affari Interni, che essendo un organo esecutivo, non può senz'altro considerarsi imparziale ed indipendente[395].

[390]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., par. 302.
[391]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania*, cit., par. 57.
[392]Corte europea dei diritti umani, *Weber e Saravia c. Germania*, cit., par. 135.
[393]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit., par. 31.
[394]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria,* cit., par. 86.
[395]*Ibidem*, par. 83.

Nel sistema legislativo del Consiglio d'Europa, l'obbligo di notifica è previsto all'articolo 2.2 della già richiamata raccomandazione R (87) del 1987 quale mezzo di controllo indipendente che l'individuo sottoposto a misure di sorveglianza ha a disposizione a posteriori per agire in maniera retroattiva e tutelarsi contro eventuali abusi. Inoltre, dato il particolare momento storico che la comunità internazionale sta attraversando e le sempre più invasive politiche di contrasto al terrorismo internazionale, la necessità di prevedere un efficace ed indipendente controllo giurisdizionale è stata anche più recentemente ribadita nei rapporti adottati dallo *Special Rapporteur* sul diritto alla privacy – già oggetto di analisi nel primo capitolo del presente elaborato[396]. In particolare, nel rapporto pubblicato a febbraio 2017, J. Cannatacci sottolineava che "[…] that better thought-out and better resourced oversight of intelligence activities is one of the many complementary initiatives that may help improve the protection of the right to privacy world-wide[…]"[397].

Sulla base di questi motivi, la Corte europea dei diritti umani è giunta ad affermare, nelle due sentenze esaminate, la contrarietà all'articolo 8 CEDU delle misure di interferenza previste dalle leggi nazionali[398].

3.2.5 Il test della necessità

Oltre che per i motivi precedentemente citati, la sentenza *Roman Zakharov* può essere considerata davvero un *leading case* nell'attuale contesto europeo in materia di sorveglianza di massa dal momento che essa, al fine di accertare se le misure limitative siano necessarie in una società democratica, ha descritto in maniera dettagliata i criteri e gli standard minimi da rispettare a livello legislativo nazionale da parte di qualsiasi Stato firmatario della Convenzione. Si può ritenere inoltre che questi standard, grazie alle costanti interazioni e reciproche influenze tra la Corte europea dei diritti umani e la Corte di giustizia, siano stati fatti propri anche a livello di legislazione europea negli ultimi regolamenti e direttive in materia.

---

[396]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy,* 31esima sessione, 24 novembre 2016, A/HRC/31/64, par. 9; *Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci*, 34esima sessione, 27 febbraio-24 marzo 2017, A/HRC/34/60, parr. 25 e 38.
[397]*Ibidem*, par. 3.
[398]Corte europea dei diritti umani (GC), *Roman Zakharov c. Russia*, cit, par. 234; *Zsabo e Vissy c. Ungheria*, cit., par. 86. In dottrina cfr. P. CZECH, *Überwachungsbefugnisse der Sicherheitsbehörden zur Terrorabwehr ohne richterliche Kontrolle*, in *Österreiches Institut für Menschenrechte* 2016, pag. 45.

Nello specifico, questi standard sono l'accessibilità e la prevedibilità della legge nazionale, la natura di reati che possono giustificare il ricorso a misure di intercettazione, determinare lo scopo e la durata della misura di sorveglianza, la trasparenza delle procedure di raccolta, accesso, esame, utilizzo e distruzione dei dati personali intercettati, la possibilità di prevedere un meccanismo di notifica successiva e la previsione di possibili rimedi esperibili di fronte al giudice nazionale. In generale, si può infatti affermare che negli ultimi anni "[…] ECtHR's human rights standards – which should be considered minimum standards – have served as a benchmark for Member States' legislative reforms"[399].

In particolare, il requisito della legittimità risulta strettamente connesso con quello della necessità nella misura in cui, in base anche quanto affermato dalla Corte europea dei diritti umani, la qualità della legge deve essere valutata non solo con riferimento alla sua accessibilità e prevedibilità, ma anche in considerazione della capacità di predisporre misure di intercettazione solo nei casi davvero necessari e nel prevedere, in ogni caso, idonee garanzie contro possibili abusi[400]. Nel contesto delle misure di sorveglianza il test della necessità si riferisce generalmente alla salvaguardia della sicurezza nazionale e delle istituzioni democratiche e al connesso bisogno di acquisire informazioni di *intelligence* nelle singole operazioni[401].

I criteri sopra citati, adottati della Grande Camera per verificare la sussistenza del requisito della "necessità in una società democratica", sono poi stati ripresi nella successiva sentenza *Szabo e Vissy c. Ungheria*. In questa sentenza la Corte europea dei diritti umani aveva ritenuto infatti che, mentre era pacifico che le misure limitative del diritto alla protezione dei dati personali perseguissero il fine legittimo di prevenire attacchi terroristici e garantire l'ordine pubblico[402], la legge ungherese non risultava sufficientemente dettagliata sia sotto il profilo dell'indicazione dei criteri in base ai quali identificare i possibili destinatari delle intercettazioni[403], sia in merito alla previsione di un obbligo di motivare l'adozione delle suddette misure[404]. Inoltre, la mancanza di un

[399]Corte europea dei diritti umani (CG), *Roman Zakharov c. Russia*, cit., par. 231. Cfr. anche Report FRA *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update,* cit., pag. 20.
[400]Corte europea dei diritti umani (CG), *Roman Zakharov c. Russia*, cit., par. 236.
[401]Corte europea dei diritti umani, *Szabo e Vissy c. Ungheria*, opinione concorrente del Pinto de Albuquerque, cit., par. 21.
[402]*Ibidem,* par. 55.
[403]*Ibidem*, parr. 66 e 67.
[404]*Ibidem,* par. 71.

preventivo controllo giurisdizionale lasciava alle autorità di sicurezza e di polizia un ampio margine di discrezionalità sia nel decidere la portata che i destinatari delle misure di interferenza[405].

In questo contesto, i giudici di Strasburgo richiamano ampiamente la decisione della Corte di giustizia nel caso *Digital Rights Ireland Ltd* e il rapporto dello *Special Rapporteur* delle Nazioni Unite Frank La Rue sulla promozione e la protezione della libertà di opinione ed espressione in merito alla possibilità di restringere il diritto alla privacy soltanto nei limiti di quanto strettamente necessario[406].

3.2.6 La separazione tra il potere giudiziario e il potere legislativo

In generale, si può affermare che la maggior parte delle violazioni riconosciute dalla Corte europea dei diritti umani ai diritti sanciti dalla CEDU sia dovuta ad abusi di potere da parte delle autorità statali; questo rischio diventa ancora più concreto nel caso di misure di sorveglianza, che per definizione vengono adottate per lo più da organi esecutivi, senza previa autorizzazione giudiziaria e in assoluta segretezza.
In questo contesto diventa pertanto fondamentale, al fine di evitare che un organo ecceda le proprie competenze, che vi sia a livello nazionale una netta e ben definita separazione fra il potere legislativo, il quale definisce, attraverso le leggi, le condizioni sostanziali e procedurali necessarie per disporre legittimamente le misure di intercettazione, il potere esecutivo, che nel concreto applica le misure e, infine, il potere giudiziario, che ha il compito si verificare in via preventiva e, qualora ciò non fosse possibile, in maniera successiva, la sussistenza dei requisiti richiesti dalla legge e il corretto operare degli organi legislativo ed esecutivo.

[405] *Ibidem,* par. 73.
[406] *Ibidem*, parr. 23 e 24.

3.3 VERSO UN SISTEMA EUROPEO UNIFORME IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Dall'analisi delle sentenze rese dalla Corte di giustizia e della Corte europea dei diritti umani sono emersi alcuni tratti comuni e ricorrenti in materia di protezione dei dati personali, i quali possono rappresentare le basi per la creazione di un sistema di tutela comune in ambito europeo. La definizione di standard comuni diventa ancora più importante se si considera anche che, in base a quanto stabilito nel caso *Maximilian Schrems*, le informazioni personali possono essere trasferite solo a quei paesi terzi che garantiscono un livello di protezione "essenzialmente equivalente" a quello riconosciuto a livello europeo[407].
In particolare, è pacificamente riconosciuto da entrambi gli organi giurisdizionali che le limitazioni al suddetto diritto, sancito rispettivamente dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea e dall'articolo 8 CEDU, possano avere luogo solo qualora siano previste dalla legge, siano necessarie in una società democratica, perseguano un fine legittimo e siano proporzionate.

Merita soffermarsi, inoltre, sul principio di proporzionalità. Invero, una delle importanti sfide future di tutto il sistema internazionale ed europeo di tutela dei diritti umani è rappresentata proprio dalla necessità di trovare un giusto bilanciamento tra i bisogni e i diritti dei singoli, da un lato, e gli interessi collettivi e di tutela della sicurezza nazionale, dall'altro lato. Questa esigenza deve essere tradotta, in termini pratici, con l'adozione di misure legislative proporzionate. Il principio di proporzionalità può essere infatti definito come un elemento di costituzionalismo globale necessario per valutare la correttezza delle limitazioni ai diritti poste in essere da soggetti per lo più pubblici[408]. Esso è divenuto, nel corso degli anni, un principio generale del diritto dell'Unione europea e, allo stesso tempo, uno dei criteri di valutazione della compatibilità delle restrizioni ai diritti umani sanciti dalla CEDU nella giurisprudenza della Corte europea dei diritti umani[409].
Per quanto riguarda la Corte di giustizia, essa utilizza il principio di proporzionalità per

[407]F. BOEHM, *op. cit.*, v. sopra nota 234, pag. 179.
[408]Cfr. F. FONTANELLI, *The mythology of Proportionality in Judgements of the Court of Justice of the European Union on Internet and Fundamental Rights*, in *Oxford Journal of Legal Studies* 2016, pag. 14.
[409]Cfr. T.I. HARBO, *The Function of the Proportionality Principle in EU Law*, in *European Law Journal* 2010, pagg. 171-173.

interpretare inizialmente la direttiva 95/46/CE. In particolare, è su questo concetto che i giudici valutano l'estensione del diritto in capo agli individui e la possibilità di raccogliere e trattare i dati personali per le finalità più diverse[410].

A riguardo è importante evidenziare il caso *Österreichischer Rundfunk*[411], in cui la Corte di giustizia veniva chiamata a decidere in merito alla compatibilità con il diritto comunitario della normativa austriaca, che imponeva agli enti di diritto pubblico soggetti al controllo della Corte dei conti di comunicare a quest'ultima i nomi e gli stipendi e le pensioni dei dipendenti che superavano una certa soglia di reddito. Nella suddetta pronuncia i giudici di Lussemburgo, una volta stabilito che le informazioni relative al reddito dei dipendenti dovessero essere considerate dati personali ai sensi della direttiva 95/46/CE, invocavano la necessità di interpretare quest'ultima alla luce dell'articolo 8 CEDU[412]. In particolare, la Corte di giustizia riteneva di dovere accertare se la disposizione austriaca in esame fosse compatibile con l'articolo 8 CEDU sotto il profilo della proporzionalità[413] e concludeva attribuendo al giudice del rinvio il compito di accertare che le misure limitative alla protezione dei dati personali fossero proporzionate e necessarie all'obiettivo di buona gestione delle risorse pubbliche.

Inoltre preme qui evidenziare, quale ulteriore elemento di prova a favore della stretta interconnessione che sussiste tra il sistema europeo e il sistema CEDU in materia di protezione dei dati personali anche prima del Trattato di Lisbona, quanto stabilito al paragrafo 91 della sentenza in esame secondo cui "Se i giudici del rinvio concludono nel senso dell'incompatibilità della normativa nazionale di cui trattasi con l'art. 8 della CEDU, tale normativa non può soddisfare neanche il requisito di proporzionalità contenuto agli artt. 6, n. 1, lett. c), e 7, lett. c) o e), della direttiva 95/46".

È proprio sulla base del principio di proporzionalità che nel 2014 è stata annullata nel caso *Digital Rights Ireland Ltd* la cosiddetta "Data Retention Directive"[414], in quanto non conforme alla Carta dei diritti fondamentali dell'Unione europea. Ivi la Corte di giustizia ha infatti ritenuto necessario valutare la discrezionalità del legislatore europeo con riferimento al "settore interessato, la natura del diritto di cui trattasi garantito dalla Carta,

[410]Cfr. C. B. TRANBERG, *Proportionality and data protection in the case law of the European Court of Justice,* in *International Data Protection Law* 2011*,* pag. 239.
[411]Corte di giustizia, *Rechnungshof c. Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann c. Österreichscher Rundfunk,* cit.
[412]*Ibidem*, parr. 19 e 21.
[413]*Ibidem*, parr. 86 e 88.
[414]Direttiva 2006/24/CE.

la natura e la gravità dell'ingerenza nonché le finalità di quest'ultima"[415]. Nel caso di specie, data l'importanza fondamentale assunta dalla protezione dei dati personali, il potere di discrezionalità andava interpretato in maniera restrittiva.

In maniera analoga a quanto statuito nei casi *Roman Zakharov c. Russia* e *Zsabo e Vissy c. Ungheria*, anche nei casi della Corte di giustizia *Digital Rights Ireland Ltd* e *Tele2 Sverige AB,* veniva stabilito che le misure europee e nazionali dovessero indicare le modalità con cui i dati personali potevano essere raccolti ed utilizzati dalle autorità di polizia e sicurezza, prevedere delle specifiche norme che disciplinavano il controllo preventivo da parte del giudice e rinforzare l'istituto della notifica successiva al fine di tutelare l'individuo contro possibili abusi[416].

In conclusione, si può affermare che il ruolo svolto dalla Corte europea dei diritti umani e dalla Corte di giustizia in questo contesto sia estremamente significativo. Entrambi gli organi giurisdizionali hanno infatti contribuito in maniera differente ad innalzare gli standard minimi di tutela dei dati personali degli individui. Invero, mentre i giudici di Lussemburgo, non avendo competenza a giudicare le legislazioni nazionali degli Stati membri, si sono preoccupati di definire i limiti all'utilizzo e al flusso di dati verso Paesi terzi, dichiarando l'accordo con gli Stati Uniti "Safe Harbour" invalido, quelli di Strasburgo hanno imposto agli stati membri CEDU gli standard minimi da rispettare in materia di misure di sorveglianza ed intercettazione.

Si può inoltre rilevare che inizialmente la Corte di giustizia si limitava a giudicare la compatibilità della normativa comunitaria con la direttiva 95/46/CE e la Carta dei diritti fondamentali dell'Unione europea, mentre, in tempi più recenti, ha iniziato ad utilizzare anche quale parametro di riferimento l'articolo 8 CEDU. Lo stesso dicasi per la Corte europea dei diritti umani nei confronti della Carta dei diritti fondamentali dell'Unione europea.

Si possono ritenere standard comuni ai due sistemi di tutela dei diritti umani le specifiche regole sui dati personali sensibili e sul trasferimento dei dati a Paesi terzi, la previsione di un'autorità di controllo indipendente e imparziale, il controllo giurisdizionale successivo e l'obbligo di notifica, il principio di proporzionalità e, infine, le regole sulle decisioni automatiche e la sicurezza dei dati. Tutti questi standard devono essere rispettati in

[415]Corte di giustizia (Grande Sezione), *Digital Rights Ireland Ltd*, cit., par. 47.
[416]Cfr. C. JASSERAND, *op. cit.,* v. sopra nota 284, pag. 160.

maniera cumulativa e le restrizioni ai diritti sono ammesse soltanto nei limiti di quanto strettamente necessario e sempre nel rispetto del principio di proporzionalità.

Il fenomeno dei richiami fra organi giurisdizionali non è nuovo nel panorama del diritto internazionale dei diritti umani, riscontrando il primo episodio già nel 1996 con il caso *P. c. S. e Cornwall County Council*[417]. Secondo parte della dottrina, inoltre, le interazioni e i continui richiami operati soprattutto dalla Corte di giustizia alla giurisprudenza della Corte europea dei diritti umani si giustificherebbero alla luce dell'articolo 52, par. 3, della Carta dei diritti fondamentali dell'Unione europea[418]. In base alla suddetta disposizione, infatti, qualora la Carta contenga diritti corrispondenti a quelli garantiti dalla CEDU, questi devono essere interpretati in base alla portata e al significato attribuite loro dalla Convenzione stessa, salvo la possibilità per il diritto dell'Unione europea di prevedere una protezione più ampia. I richiami alla giurisprudenza della Corte europea dei diritti umani servirebbero, quindi, ad evitare i possibili conflitti che potrebbero sorgere tra i due organi giurisdizionali anche alla luce della suddetta norma[419].

In generale, si può ritenere che i suddetti richiami svolgano principalmente cinque funzioni, ossia di tipo sostanziale, autoritativa, di legittimità – che può essere a sua volta ulteriormente suddivisa in tre sotto-funzioni, ossia di guida, conformità alla legittimità e avvertimento agli Stati membri in caso di possibile minaccia alla giurisprudenza di Strasburgo, o come metodo di comparazione tra la giurisprudenza della Corte europea dei diritti umani e quella della Corte di giustizia - "per analogia" e, infine, meramente decorativa. Al primo tipo di rinvio, che si esprime nel richiamare letteralmente il contenuto di una sentenza della Corte europea dei diritti umani per decidere in merito ad un rinvio pregiudiziale, appartengono all'incirca il 20% del totale delle sentenze richiamate, la maggior parte delle quali riguardano gli articoli 6 e 8 della CEDU.[420]. Per quanto riguarda, in particolare, l'articolo 8 CEDU, il primo richiamo al diritto alla privacy risale al caso

[417]Corte di giustizia, *P. c. S. Cornwall County Council*, sentenza del 30 aprile 1996, C-13/94.
[418]Cfr. J.F. BARRETT, *Convergence, Compatibility or Decoration: The Luxembourg Court's References to Strasbourg Case Law in its Final Judgments*, in *Pécs Journal of International and European Law* 2016, pag. 38.
[419]Cfr. L. SCHEECK, *Solving Europe's Binary Human Rights Puzzle. The Interaction between Supranational Courts as a Parameter of European Governance*, Questions de Recherche / Research in Question N° 15 – October 2005, disponibile alla pagina http://www.ceri-sciences-po.org/publica/qdr.htm., pag. 20.
[420]Cfr. J.F. BARRETT, *op. cit.*, v. sopra nota 418, pag. 54.

Lisa Jacqueline Grant c. South-West Trains Ltd[421] relativo all'equo trattamento lavorativo fra uomini e donne[422]. Ivi la Corte di giustizia ha infatti fatto riferimento alla giurisprudenza di Strasburgo per affermare che due persone dello stesso sesso, non coniugate ma legate da una relazione stabile, non possano considerarsi membri di una famiglia in base alla nozione prevista dall'articolo 8 CEDU[423]. Nei successivi casi *Roquette*[424] e *Hoechst*[425] i giudici di Lussemburgo non si limitano a richiamare la giurisprudenza CEDU, ma allineano le loro sentenze con essa. In altri casi, invece, i richiami servono quali basi di legittimità delle sentenze dei giudici di Lussemburgo, in particolare sotto il profilo della loro compatibilità con la tutela dei diritti fondamentali nel sistema europeo. Ma la funzione in assoluto maggiormente utilizzata è quella di "guida"[426], così si ha avuto modo di analizzare nel caso *Österreicher Rundfunk* con riferimento al principio di proporzionalità. Nel contesto del diritto alla privacy, infatti, "[…] Strasbourg case law has become a hermeneutical tool for the Luxembourg judges' interpretation of legal definitions and examinations of the scope of fundamental rights"[427].

Occorre, inoltre, avere riguardo al diverso ruolo svolto rispettivamente dalla Corte di giustizia e dalla Corte europea dei diritti umani nei confronti del sistema giuridico nazionale. Questo determina infatti le modalità e i limiti con cui le decisioni giurisdizionali sono recepite dagli Stati membri. Per quanto riguarda il diritto dell'Unione europea, in base al principio del primato del diritto comunitario sul diritto interno, le decisioni della Corte di giustizia hanno efficacia diretta negli ordinamenti nazionali e prevalgono anche sulla normativa nazionale con esse contrastante, che dovrà quindi, qualora necessario, venire disapplicata.

Per contro la CEDU, pur essendo stata prevista esplicitamente dall'articolo 6, par. 2,

---

[421]Corte di giustizia, *Lisa Jacqueline Grant c. South-West Trains Ltd*, sentenza del 17 febbraio 1998, C-249/96.

[422]La Corte di giustizia richiama, in particolare, al paragrafo 33, i casi della Corte europea dei diritti umani, *X. e Y. C. Regno Unito*, sentenza del 3 maggio 1983, ricorso n. 9369/81, Commissione europea dei diritti umani, *S. c. Regno Unito*, sentenza del 14 maggio 1986, ricorso n. 11716/85 e Corte europea dei diritti umani, *Kerkhoven e Hinke c. Paesi Bassi*, sentenza del 19 maggio 1992, ricorso n. 15666/89.

[423]Corte di giustizia, *Lisa Jacqueline Grant,* cit.*,* par. 33.

[424]Corte di giustizia, *Roquette Frères SA c. Directeur général de la concurrence, de la consommation et de la répression des fraudes*, con l'intervento della Commissione delle Comunità europee, sentenza del 22 ottobre 2002, C-94/00.

[425]Corte di giustizia, *Hoechst AG c. Commissione delle Comunità europee*, sentenza del 21 settembre 1989, cause riunite C-46/87 e C-227/88.

[426]J.F. BARRETT, *op. cit.,* v. sopra nota 418, pag. 62.

[427]*Ibidem*.

TUE[428] la possibilità per l'Unione europea di aderirvi – il che comporterebbe per la stessa la pari equiparazione ai Trattati – il relativo processo si è interrotto in seguito al parere negativo reso dalla Corte di giustizia nel 2014[429], per cui la CEDU continua ad essere priva di efficacia diretta e assume il valore attribuitole di volta in volta da ciascun ordinamento interno degli Stati membri. Per quanto riguarda, ad esempio, il sistema legislativo italiano, essa ha assunto, in seguito a diverse pronunce costituzionali, il valore di parametro interposto ex articolo 117 Cost[430].
Non avendo la competenza per annullare in maniera diretta le norme nazionali, la Corte europea dei diritti umani, anche in ragione del suo ruolo preminentemente sussidiario, garantisce il rispetto dei diritti sanciti dalla CEDU tramite i principi sanciti nelle sue sentenze, alle quali i giudici sono tenuti a conformarsi nell'interpretare delle leggi interne[431].

A livello storico, prima dell'entrata in vigore del Trattato di Lisbona, solo la Corte di giustizia operava i rinvii nei confronti della giurisprudenza della Corte europea dei diritti umani, considerata quest'ultima l'unico organo competente a giudicare in materia di diritti umani. Si riscontrano, infatti, all'incirca una cinquantina di richiami, dovuti soprattutto alla mancanza di sufficientemente giurisprudenza della Corte di giustizia per interpretare in maniera corretta i casi che avevano ad oggetto la tutela dei diritti fondamentali. Il numero dei rinvii è diminuito in seguito all'entrata in vigore del Trattato di Lisbona e al riconoscimento della Carta di Nizza di pari valore dei trattati. Se da un lato, quindi, il richiamo alle pronunce dei giudici di Strasburgo da parte di quelli di Lussemburgo è un fenomeno ormai consolidato da decenni, è interessante riscontrare come, invece, la Corte europea dei diritti umani abbiano iniziato solo negli ultimi anni ad agire in maniera analoga. Invero, la Corte di giustizia è tenuta a fare riferimento alla giurisprudenza CEDU in ragione di quanto previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea. Per contro, nessun obbligo sussiste in capo ai giudici di Strasburgo. A detta di chi scrive, la mancanza di un suddetto obbligo si manifesta nel fatto che, nelle sentenze della Corte europea dei diritti umani, i richiami alla giurisprudenza della Corte di

[428]Articolo 6, par. 2, TUE "L'Unione aderisce alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Tale adesione non modifica le competenze dell'Unione definite nei trattati".
[429]Corte di giustizia (Plenaria), *parere 2/13,*18 dicembre 2014.
[430]I suddetti principi sono stati sanciti nelle "sentenze gemelle", nn. 348/07 e 349/07 della Corte Costituzionale italiana.
[431]J.F. BARRETT, *op. cit.*, v. sopra nota 418, pag. 38.

giustizia, cui sono spesso dedicati anche un numero consistente di pagine, restino però sempre rilegati alla parte iniziale del ragionamento della Corte, ossia citati affianco alle fonti di diritto internazionale o dell'Unione europea, di cui la Corte si avvale, ma che non è obbligata a rispettare, nella propria decisione finale.

In realtà, secondo parte della dottrina, la quale fonda le proprie considerazioni sul dettato normativo e, in particolare, sull'*explanation report* relativo alla Carta dei diritti fondamentali dell'Unione europea, l'articolo 8 CEDU sarebbe solo riprodotto all'interno dell'articolo 7, ossia con riferimento alla protezione della vita privata e familiare, e non, invece, nell'articolo 8 relativo al diritto alla protezione dei dati personali. Conseguentemente, l'articolo 52 non troverebbe applicazione tutte le volte in cui la Corte di Lussemburgo è chiamata a giudicare in materia di dati personali. A detta di chi scrive, questa tesi non appare pienamente condivisibile, soprattutto alla luce di quanto stabilito nel considerando 11 della direttiva 95/46/CE, che già espressamente richiamava alla Convenzione 108:"Considerando che i principi della tutela dei diritti e delle libertà delle persone, in particolare del rispetto della vita privata, contenuti dalla presente direttiva precisano ed ampliano quelli enunciati dalla convenzione del 28 gennaio 1981 del Consiglio d'Europa sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale". La suddetta tesi è stata inoltre confermata dall'Avvocato Generale Pedro Cruz Villanón nella sua opinione relativa al caso *Scarlet Extended SA c. Société belge des auteurs compositeurs et éditeurs (Sabam*): "pertanto, e con le riserve espresse in precedenza, propongo di modificare la questione del giudice del rinvio sostituendo il riferimento agli artt. 8 e 10 della CEDU con quello agli «artt. 7, 8 e 11 della Carta, in combinato con l'art. 52, n. 1, della stessa, come interpretati, ove necessario, alla luce degli artt. 8 e 10 della CEDU"[432].

Infine, quale ulteriore elemento a conferma di un costante, e reciprocamente connesso, dialogo fra i giudici di Strasburgo e Lussemburgo, viene in rilievo l'utilizzo da parte di questi ultimi del margine di apprezzamento, tipico del sistema giurisprudenziale CEDU, ogniqualvolta vengano in gioco da un lato una libertà comunitaria e, dall'altro lato, un diritto fondamentale dell'individuo. Per un'analisi più approfondita di questo aspetto si rinvia a quanto già precedentemente esposto nel paragrafo 3.1.1. del presente elaborato.

[432]Corte di giustizia, *Scarlet Extended SA contro Société belge des auteurs compositeurs et éditeurs (Sabam)*, Conclusioni Dell'avvocato Generale Pedro Cruz Villalón presentate il 14 aprile 2011, C-70/10, par. 34.

CAPITOLO 4
QUESTIONI IRRISOLTE IN MATERIA DI TUTELA INTERNAZIONALE DEI DEL DIRITTO ALLA PROTEZIONE DEI DATI PERSONALI

4.1 NUOVI PROFILI DI RESPONSABILITA' 4.1.1 La protezione dei dati personali: diritto pubblico o diritto privato? 4.1.2 Il ruolo degli *Internet service provider* nel trasferimento dei dati alle autorità di *law enforcement*. 4.1.3 Le possibili soluzioni avanzate a livello internazionale e i *Guiding Principles on Business and Human Rights* 4.1.4 L'ambito di applicazione della direttiva (UE) 2016/680: una lacuna nella tutela del singolo? 4.1.5. Il crescente ruolo assunto dagli *Internet service provider* nella giurisprudenza della Corte di giustizia e della Corte europea dei diritti umani. 4.2. L'ESERCIZIO EXTRATERRITORIALE DELLA GIURISDIZIONE E LA TUTELA DEI DIRITTI UMANI 4.2.1. L'esercizio extraterritoriale della giurisdizione in caso di esercizio della facoltà di deroga prevista dal Patto sui diritti civili e politici e dalla CEDU. 4.2.2. L'applicazione extraterritoriale del regolamento (UE) 2016/679 e la compatibilità con i principi sanciti dal diritto internazionale consuetudinario. 4.2.3. Come riconciliare l'universalità di Internet e il principio territoriale della giurisdizione? Il principio degli effetti come possibile soluzione.

4.1 NUOVI PROFILI DI RESPONSABILITÀ

Nel terzo capitolo sono state analizzate le principali problematiche affrontate dalla Corte europea dei diritti umani e dalla Corte di giustizia negli ultimi anni in materia di tutela dei dati personali, focalizzandosi, in particolare, sulle interazioni fra i due organi giurisdizionali – che sembrerebbero far propendere verso la creazione di un "dialogo fra Corti" anche in questo contesto – e sulla maggiore propensione da parte dei giudici di Strasburgo ad accogliere anche i cosiddetti ricorsi "in astratto", date le maggiori difficoltà riscontrate per i ricorrenti nel dimostrare di essere i diretti destinatari di misure di sorveglianza ed intercettazione, in ragione della natura spesso segreta delle stesse. Inoltre, sempre secondo la Corte europea dei diritti umani, e come più volte evidenziato anche nei diversi rapporti dello *Special Rapporteur* Cannatacci, in caso di misure di interferenza con il diritto alla privacy è necessario implementare il meccanismo della notifica successiva, al fine di facilitare agli individui i ricorsi dinanzi ai competenti organi giurisdizionali in caso presunte violazioni dell'articolo 8 CEDU.

Tuttavia, restano ancora irrisolte alcune questioni, su cui né la Corte europea dei diritti umani né altri organi internazionali di controllo hanno ancora avuto modo di pronunciarsi, relative soprattutto all'eventuale applicazione extraterritoriale della Convenzione in caso di violazione degli articoli 8 CEDU e 17 del Patto sui diritti civili e politici, e all'eventuale imputazione di responsabilità da parte dei soggetti privati, che operano sempre più in stretta connessione con le autorità statali preposte alle attività di *law enforcement* e sicurezza nazionale e alle quali trasmettono ingenti quantità di dati personali. Sotto quest'ultimo profilo, infatti, essendo i ricorsi di fronte ai diversi organi internazionali di controllo limitati alle sole violazioni poste in essere da organi statali, si ravvisa una lacuna nella tutela dei diritti degli individui tutte le volte in cui la privacy viene

violata da atti compiuti nel concreto da società, ma spesso indirettamente attribuibili agli Stati.

Pertanto, permangono in questo contesto numerose aree di incertezza - dovute anche al venire meno della separazione fra diritto pubblico e diritto privato - che si cercherà in questo capitolo, per quanto possibile, di chiarificare, utilizzando gli strumenti già a disposizione dal diritto internazionale dei diritti umani e dal diritto europeo in materia di tutela dei diritti umani, al fine di prospettare eventuali ipotesi risolutive.

Si procederà, innanzitutto, ad un'analisi dei problemi legati all'eventuale imputazione di responsabilità nei confronti delle società private in caso di violazione del diritto umano alla protezione dei dati personali e poi, successivamente, ci si focalizzerà sugli aspetti legati alla possibile applicazione extraterritoriale della CEDU e del Patto sui diritti civili e politici.

Per quanto concerne la metodologia, questo capitolo si svilupperà, in maniera analoga a quanto già svolto nei paragrafi precedenti dedicati alle fonti normative che tutelano il diritto alla protezione dei dati personali, partendo da un'analisi della problematica da un punto di vista più ampio – evidenziando le soluzioni avanzate dagli organi di controllo di diritto internazionale – per poi passare ad un livello più circoscritto, ossia quello regionale, focalizzandosi, principalmente, sulle questioni controverse affrontate a livello legislativo europeo e nel sistema di tutela previsto dalla CEDU. Invero, la mancanza di un adeguato sistema di responsabilità nei confronti delle società di diritto privato farebbe propendere, sia a livello internazionale che regionale, verso l'adozione di criteri principalmente preventivi piuttosto che successivi. Allo stesso tempo, anche la Corte europea ha dimostrato una maggiore apertura a fare valere le ragioni del singolo in caso di violazione del diritto alla privacy da parte delle società di diritto privato, sulla base degli obblighi positivi gravanti in capo agli Stati in base all'articolo 8 CEDU.

A riguardo, si rileva come l'attuazione delle diverse misure di sorveglianza di massa, poste in essere dai governi statali per ragioni di sicurezza nazionale e, in particolare, per contrastare il fenomeno del terrorismo internazionale, venga sempre maggiormente demandata a soggetti privati. Questa pratica viene tradizionalmente

chiamata "Privatized counter-terrorist surveillance" e indicata con l'acronimo PCTS[433]. Com'è facilmente intuibile, la privatizzazione delle suddette misure ha dato origine a numerose problematiche, legate soprattutto all'imputazione di responsabilità nei confronti delle società in caso di violazione della privacy e alla tutela che le persone fisiche lese possono ricevere sia nel proprio ordinamento che in quello internazionale o regionale.
Il diffondersi della tecnologia e dei mezzi di informazione, ma soprattutto dei cosiddetti telefoni cellulare "smartphones", ha permesso una diffusione di dati personali senza precedenti e ha agevolato le possibilità per i governi statali di immagazzinare i suddetti dati, usufruendo anche di soggetti privati di diritto. Questi ultimi, inoltre, a differenza delle autorità pubbliche che esercitano i propri poteri nel rispetto e nei limiti delle leggi e delle Costituzioni, non sono soggetti ad alcuna limitazione di sorta e, anzi, sono gli stessi individui a cedere loro una larga quantità di privacy e libertà personale accettandone i relativi termini e condizioni.

4.1.1 La protezione dei dati personali: diritto pubblico o diritto privato?

Quella della protezione dei dati personali costituisce una materia in cui la distinzione tra diritto pubblico e diritto privato può risultare labile. Ciononostante, ricollegarla all'una o all'altra categoria comporta importanti conseguenze, relative soprattutto all'esercizio della giurisdizione e al diritto applicabile. Infatti, considerare la materia come di diritto pubblico implica l'impossibilità per gli organi giurisdizionali stranieri di applicare qualsiasi legislazione straniera in base ai criteri stabiliti ad esempio, per quanto riguarda il contesto europeo, dal Regolamento Bruxelles I *bis*[434], ipotesi, invece, contemplata in caso di controversie tra privati. La difficoltà, e forse addirittura l'impossibilità, di classificare in maniera definita il diritto alla protezione dei dati personali come pubblico o privato deriva principalmente dalla pluralità di fonti che hanno originato l'odierno sistema di tutela, il quale ha recepito istituti tipici del diritto internazionale di tutela dei diritti umani, del diritto civile, del diritto dei consumatori e tanti altri.

Una possibile soluzione al problema potrebbe essere indagare la natura delle autorità che hanno raccolto e trattato i dati personali, pubbliche e di polizia in un caso, soggetti di

[433]Cfr. F. DE LONDRAS, *Privatized counter-terrorist surveillance*, in F. DAVIS, N. MC. GARRITY, G. WILLIAMS, *Surveillance, Counter-Terrorism and Comparative Constitutionalism,* Routledge, Londra 2013, pagg. 59 e ss.
[434]Regolamento (UE) 2012/1215.

diritto privato nell'altro caso. Il criterio di classificazione si baserebbe, pertanto, non sull'attività svolta in sé, ma sul soggetto preposto alla stessa[435]. Orbene, anche questo criterio non sembra essere però totalmente risolutivo, anche alla luce delle criticità messe in evidenza nel paragrafo precedente relative alla cooperazione fra tra le società private e le autorità statali per la raccolta dei dati per finalità di *law enforcement* e alle incertezze tuttora esistenti in merito all'applicazione della direttiva (UE) 2016/680 o del regolamento (UE) 2016/679. Si consideri, inoltre, che anche il suddetto regolamento si applica sia al settore pubblico che a quello privato, grazie all'articolo 37 che disciplina i casi in cui il titolare del trattamento o il responsabile del trattamento siano un'autorità o un organismo pubblico[436].

4.1.2 Il ruolo degli *Internet service provider* nel trasferimento dei dati alle autorità di *law enforcement*

Di seguito vengono riportati in grafico i risultati dell'analisi condotta sui dati richiesti negli ultimi anni dalle autorità di *law enforcement* alle principali società coinvolte nel programma di sorveglianza statunitense PRISM denunciato da Edward Snowden. Vengono riportati, in particolare, i dati resi pubblici nei cosiddetti "trasparency report" delle principali società coinvolte nello scandalo del *data gate*, ossia Microsoft, Google, Facebook, Oath e Apple. Si è deciso, inoltre, di riportare i dati relativi a Twitter, in ragione dell'estesa diffusione dell'*Internet service provider* in tutto il mondo, che conta ad oggi più di 330 milioni di utenti.

I suddetti rapporti vengono tipicamente pubblicati sulle pagine *web* delle società che forniscono servizi di comunicazione e sono divisi in diverse sezioni, a seconda dell'area geografica e dell'anno solare di riferimento. La pubblicazione sempre più diffusa di questi rapporti da parte delle società che operano sul *web* costituisce un segnale positivo di una crescente tendenza a voler garantire una maggiore trasparenza in merito alle informazioni raccolte dagli utenti.

Il grafico indica sulla linea verticale la quantità di dati diffusi, con soglie numeriche divise in decine di migliaia, mentre sulla linea orizzontale sono indicati gli anni solari di

[435]Cfr. U. KOHL, *Jurisdiction and the Internet*, Regulatory Competence over Online Activity, Cambridge University Press 2007, pag. 230.
[436]Articolo 37 regolamento (UE) 2016/679.

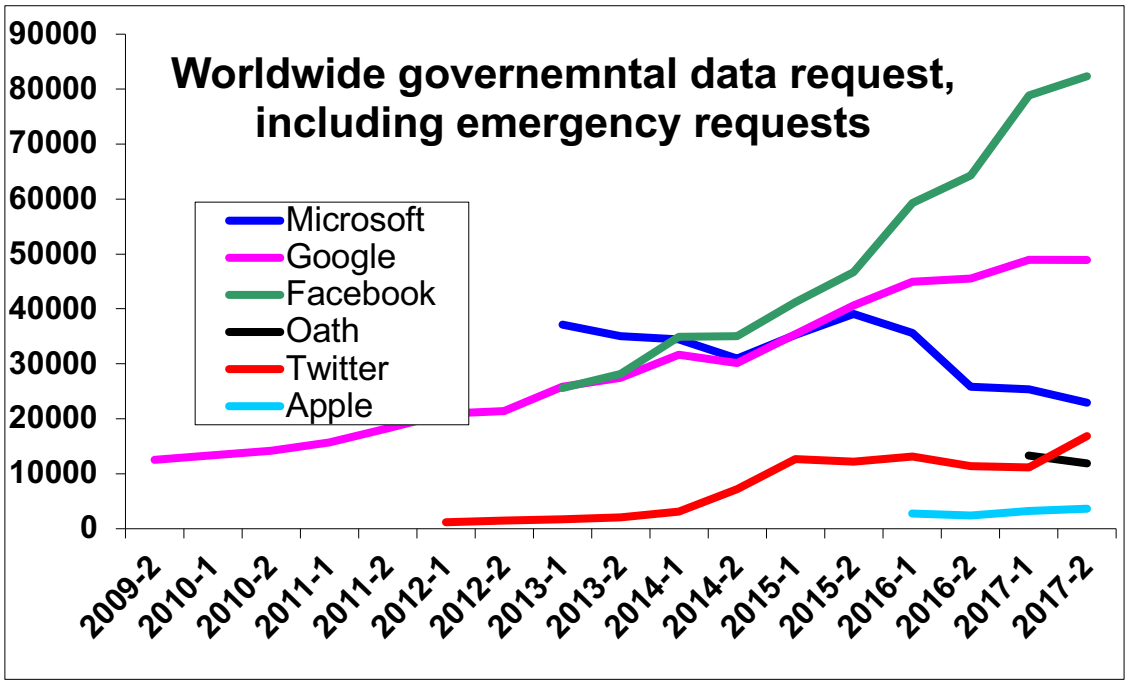
riferimento, a partire dall'anno in cui le società di riferimento hanno iniziato a redigere i rapporti.

Dal punto di vista metodologico, si è deciso di analizzare sia i dati trasmessi in condizioni normali, in seguito cioè ad un mandato o ad una richiesta di prova, sia quelli trasmessi in situazioni di emergenza, senza la necessità di alcuna autorizzazione giudiziaria.

Inoltre, le informazioni raccolte e trasmesse sono riconducibili sia alla categoria dei *non-content data*, ossia delle informazioni relative al nome, cognome e indirizzo, contatti, indirizzo di posta elettronica degli utenti, indirizzo IP, la localizzazione, sia ai cosiddetti *content data*, ossia i dati relativi al contenuto delle conversazioni che è stato possibile creare grazie ai servizi offerti dalle società in oggetto.

Nella presente analisi non sono state prese in considerazione le richieste di dati presentate dal governo statunitense in base al *Freedom Act* - cui i rapporti dedicano un'apposita sezione - essendo quest'ultimo riconducibile all'ambito della sicurezza nazionale americana, non oggetto del presente elaborato.

Occorre, infine, evidenziare che alcune società, tra cui ad esempio Apple, prevedono il sistema di notifica all'utente in caso di richieste da parte delle autorità di *law enforcement*[437], salvo i casi in cui la notifica sia esplicitamente vietata dalla legge nazionale.



[437]https://www.apple.com/legal/privacy/transparency/requests-2017-H1-en.pdf.

Tabella

	Microsoft	Google	Facebook	Oath	Twitter	Apple
2009-2		12539				
2010-1		13424				
2010-2		14201				
2011-1		15744				
2011-2		18257				
2012-1		20938			1181	
2012-2		21389			1433	
2013-1	37196	25879	25607		1697	
2013-2	35083	27477	28147		2121	
2014-1	34494	31698	34946		3131	
2014-2	31002	30140	35051		7144	
2015-1	35228	35365	41214		12711	
2015-2	39083	40677	46710		12176	
2016-1	35572	44943	59229		13152	2735
2016-2	25837	45550	64279		11417	2409
2017-1	25367	48941	78890	13316	11115	3288
2017-2	22939	48877	82341	11894	16861	3648

Fonti: https://transparency.twitter.com/en/information-requests.html;
https://transparency.twitter.com/en/information-requests.html;
https://transparency.oath.com/reports/government-data-requests.html,
https://transparencyreport.google.com/user-data/overview
https://transparency.facebook.com/government-data-requests
https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/

Dall'analisi del grafico emerge un evidente incremento delle richieste di dati personali degli utenti da parte delle autorità di *law enforcement* soprattutto a partire dal secondo semestre del 2015, dovuto, verosimilmente, agli attacchi terroristici di Parigi dello stesso anno. Inoltre, Facebook risulta la società responsabile del maggiore trasferimento di dati personali alle autorità di *law enforcement*.

La questione è divenuta oggi maggiormente pressante se si considera, per esempio, l'ultimo scandalo che ha interessato la società britannica Cambridge Analytica, accusata di avere fatto uso non autorizzato dei dati personali di circa 87 milioni di utenti Facebook per le campagne elettorali negli Stati Uniti. In particolare, il 17 marzo 2018, il *New York Times* e l'emittente televisiva britannica Channel 4 News riportavano diverse dichiarazioni rese

dall'ex dipendente di Cambridge Analytica, Christopher Wylie, relative alla quantità e alla natura dei dati raccolti e a diverse informazioni scambiate fra Facebook, la società britannica e alcuni rappresentanti politici americani, che aveva assunto Cambridge Analytica per raccogliere i dati personali degli utenti ed influenzare le opinioni dei votanti. Gli ultimi scandali resi pubblici in tema di raccolta indiscriminata di dati personali hanno di fatto incoraggiato nuove riflessioni in merito agli standard etici e legali da implementare e far rispettare dalle società di *social media* e, in generale, da tutte le società che gestiscono enormi quantità di informazioni relative agli utenti.

4.1.3 Le possibile soluzioni avanzate a livello internazionale e i *Guiding Principles on Business and Human Rights*

In termini più generali, la dottrina internazionale si sta interrogando già da tempo circa la possibilità di sviluppare un sistema di responsabilità, in certi casi anche condivisa, per gli atti illeciti compiuti da attori non statali, o da autorità statali in collaborazione con autorità non statali. La problematica risulta infatti nota già da tempo anche in contesti diversi da quello della protezione dei dati personali, quali, ad esempio, quello della responsabilità delle società private per danni ambientali o violazioni di altri diritti umani, oppure in caso di collaborazione di entità strutturate, ma non statali, per il compimento di atti terroristici. Nessuna di queste ipotesi è, infatti, contemplata nel documento internazionale in materia di illeciti internazionali, ossia nel Progetto di articoli sulla responsabilità degli Stati redatto dalla Commissione del diritto internazionale nel 2001[438], che si limita a disciplinare agli articoli 5-11 le attività illecite commesse da entità che non sono statali, ma che esercitano poteri direttamente attribuibili o svolti per conto di uno Stato. A livello legislativo, inoltre, l'estensione dell'ambito di applicazione della disciplina sulla responsabilità degli Stati per la commissione di illeciti internazionali anche alle società di diritto privato non appare priva di difficoltà, in ragione del fatto che "[…] non-state actors may differ fundamentally from states, thereby making the transposition of traditional rules of state responsibility artificial and inadequate: their loosely organised, temporary, diverse, illegitimate, or even outright criminal character may militate against applying the classic responsibility

[438]Commissione del diritto internazionale, *Responsibility of States for Internationally Wrongful Acts*, in *Official Records of the General Assembly,* 56esima sessione*, Supplement No. 10* (A/56/10).

paradigm to non-state interactions"[439]. Un ulteriore limite insormontabile potrebbe essere rappresentato dal fatto che gli attori non statali non sono tenuti a rispettare alcun obbligo previsto dal diritto internazionale, non essendo loro riconosciuta alcuna personalità giuridica in base allo stesso.

In ogni caso, in mancanza di soluzioni previste a livello di tutela internazionale dei diritti umani e all'impossibilità di applicare per analogia i criteri stabiliti in caso di illeciti internazionali commessi dagli Stati, è pur sempre possibile ricorrere, al fine di tutelare gli interessi delle parti, agli altri strumenti previsti per esempio nel diritto civile e penale nazionali. In molti casi, infatti, gli attori non statali sono società di diritto privato e quindi citabili di fronte a tribunali interni. Conseguentemente, saranno questi ultimi a decidere in merito allo loro responsabilità ed all'eventuale risarcimento del danno. Nei casi in cui, inoltre, venga constatato nelle controversie contro le società che "[…] have assisted states in the commission of wrongful acts may consider and perhaps even develop cooperative arrangements with international human rights supervisory bodies that have jurisdiction over the state which was assisted by the corporation (such body could e.g. open a *proprio motu* investigation into the state's conduct)"[440]. Al riguardo, uno degli approcci maggiormente condivisi al momento sembrerebbe essere lo "standard-setting (or regulatory) approach", tramite cui vengono appunto stabiliti degli *standard* che gli attori statali e non statali si impegnano a sottoscrivere e a rispettare, prevedendo eventualmente dei meccanismi di controllo[441]. L'adozione degli standard è quindi un rimedio di natura preventiva, che impedisce alle società di incorrere in eventuali responsabilità nel caso in cui si riscontri la commissione di un illecito[442]. Tuttavia, non sussistendo alcun obbligo internazionale vincolante per gli attori non statali di sottoscrivere i suddetti *standard*, né di rispettarli, potrebbe comunque darsi luogo ad una lacuna normativa in caso di violazione di certi diritti umani.

[439]Cfr. J. D'ASPREMONT, A. NOLLKAEMPER, I. PLAKOKEFALOS, C. RYNGAERT, *Sharing Responsibility Between Non-State Actors and States in International Law: Introduction,* in *Netherlands International Law Review* 2015, pag. 50
[440]*Ibidem*, pag. 60.
[441]*Ibidem*, pag. 61.
[442]Analoghi meccanismi preventivi sono previsti, ad esempio, nel diritto italiano in materia di responsabilità penale delle società ai sensi del Dlgs. 231/2001, ove la dimostrazione dell'adozione di modelli di organizzazione e di gestione idonei a prevenire i reati esonera l'ente da qualsiasi imputazione.

A tal fine, il 16 giungo 2011 il Consiglio per i diritti umani ha adottato i *Guiding Principles on Business and Human Rights*[443]. Al punto 1 viene specificato innanzitutto che, seppur gli Stati non siano in linea di massima responsabili per le violazione dei diritti umani da parte delle società private, essi, tuttavia, violano gli obblighi derivanti dal diritto internazionale tutte le volte in cui non agiscono in maniera tale da prevenire, investigare o punire le condotte illecite poste in essere dai suddetti enti[444]. Gli stessi concetti sono poi ribaditi ed ulteriormente specificati ai punti 25-27, ove viene sancito l'obbligo per gli Stati di assicurare, tramite misure giudiziarie, amministrative o legislative, o qualsiasi altro mezzo ritenuto idoneo, che le vittime di eventuali abusi abbiano diritto un rimedio effettivo attraverso dei meccanismi, anche non giudiziari, adeguati.
Per quanto riguarda, invece, la cosiddetta "corporate responsibility", ai punti 11 e 12 delle Linee Guida viene previsto l'obbligo per le società di rispettare i diritti umani così come riconosciuti dai trattati che compongono l'*International Bill of Human Rights* – di cui fanno parte la Dichiarazione universale dei diritti umani, il Patto sui diritti civili e politici con i due suoi protocolli addizionali e il Patto sui diritti economici, sociali e culturali – e dalla Dichiarazione dell'Organizzazione Internazionale del Lavoro (OIL) sui principi e i diritti fondamentali dei lavoratori, adottata a Ginevra nel 1998.

Inoltre, al fine di identificare e prevenire eventuali rischi per i diritti degli individui è necessario che le società svolgano una "human rights due diligence"[445]. Ovviamente in questo contesto il termine *due diligence* non assume lo stesso significato che potrebbe assumere, per esempio, nel diritto societario in caso di fusioni e acquisizioni - ove è strettamente connesso ad una valutazione di tipo economico - bensì sta ad indicare l'insieme di tutti i meccanismi volti ad identificare i potenziali rischi per i diritti umani connessi all'esercizio di un'attività imprenditoriale.

Occorre al riguardo sottolineare che nelle Linee Guida non è prevista alcuna specifica disposizione in materia di privacy, ma quest'ultima viene fatta rientrare nei obblighi imposti dalle Convenzioni internazionali e nello specifico dall'articolo 12 della Dichiarazione universale dei diritti umani e dall'articolo 17 del Patto sui diritti civili e politici.

---

[443]Consiglio per i diritti umani, *Guiding Principles on Business and Human Rights*, 27esima sessione, 6 luglio 2011, Risoluzione A/HRC/RES/17/4.
[444]*Ibidem*, principio n. 1.
[445]*Ibidem*, principio n. 4.

In ogni caso, ad eccezione delle Linee Guida appena analizzate che riguardano comunque la responsabilità generale delle società in caso di violazione dei diritti umani, non si rinviene ad oggi alcun altro strumento giuridico internazionale che disciplini la raccolta e la trasmissione illecita dei dati personali da parte degli organi privati. Una parziale soluzione al problema è stata fornita, ad esempio, per quanto riguarda l'ordinamento giuridico europeo, dal regolamento (UE) 2016/680 e dalla proposta di regolamento *e-privacy*[446], che prevedono rispettivamente al considerando 80 e all'articolo 3, par. 2, l'obbligo per le società che forniscono servizi di comunicazione elettronica di nominare, qualora non abbiano la propria sede stabilita nell'Unione europea, un rappresentante all'interno del suddetto territorio. Per un'analisi più approfondita della suddette norme giuridiche si fa rinvio a quanto precedentemente esposto nei paragrafi 2.1.2.1 e 2.1.2.4. del presente elaborato.

Viene in rilievo, infine, un recente rapporto di Amnesty International pubblicato nel 2016 ove viene evidenziata la mancata adozione da parte di diverse società che forniscono servizi di comunicazione elettronica degli standard minimi per proteggere i dati degli utenti da possibili attacchi cybernetici. Nel suddetto rapporto, si posiziona in cima alla classifica la società cinese Tencent, seguita da Blackberry e da Skype, ora di proprietà di Microsoft[447]. Questi standard minimi sono costituiti principalmente dalla crittografia *end-to-end*, su cui si avrà modo di tornare nell'ultimo capitolo e il cui rafforzamento costituisce una delle soluzioni maggiormente praticabili al fine di tutelare in maniera più efficace il diritto alla protezione dei dati personali degli individui.

Nel rapporto viene ribadito, inoltre, l'obbligo per le società di rispettare i diritti umani sanciti dai *Guiding Principles on Business and Human Rights*[448], indipendentemente dalla capacità dello Stato di farli rispettare attraverso l'adozione di leggi e regolamenti. Le società devono infatti identificare tutti i rischi connessi alle operazioni e devono pubblicamente impegnarsi a rispettare e a far rispettare il diritto alla privacy degli utenti, adottare delle misure per tutelarli maggiormente attraverso la crittografia e, infine, "make sure that users of these services, and the wider public, have an accurate picture of the risks

[446]Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), Commissione europea, 2017/0003 (COD)

[447]https://www.amnesty.org.nz/snapchat-skype-among-apps-not-protecting-users%E2%80%99-privacy.

[448]*Ibidem,* pag. 14.

in the use of the company's products and services, the measures taken to mitigate those risks, and the actual impact of a company's operations".

I cinque criteri applicati dalla ONG per redigere la classifica sono stati: 1) La società riconosce tramite le sue policy e procedure le minacce alla libertà di espressione e al diritto al privacy come rischi per gli utenti?; 2) La società applica la crittografia *end-to-end by default*?; 3) La società comunica ai propri utenti le minacce ai diritti alla privacy e alla libertà di espressione e come questa risponda attraverso l'utilizzo della crittografia?; 4) La società comunica le richieste di dati da parte dei governi?; 5) La società pubblica i dettagli relativi ai sistemi di crittografia?

Message Privacy Ranking: How the companies scored

COMPANY	IM SERVICES ASSESSED	1. RECOGNISES ONLINE THREATS TO HUMAN RIGHTS?	2. DEPLOYS END-TO-END ENCRYPTION AS A DEFAULT?	3. INFORMS USERS OF RISKS AND ENCRYPTION USED?	4. DISCLOSES GOVERNMENT REQUESTS FOR USER DATA?	5. PUBLISHES TECHNICAL DETAILS OF ENCRYPTION?	OVERALL SCORE /100
FACEBOOK	FB MESSENGER, WHATSAPP	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. Score 2	Yes, but only on WhatsApp, not on Messenger. Score 2	Inadequate notification within the apps, no warning in Messenger when using weaker encryption. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Yes, both apps use open source Signal protocol, provide specification. Score 3	73
APPLE	IMESSAGE, FACETIME	Yes, but no policy commitment to freedom of expression. Score 2	Yes. Score 3	Inadequate notification within the apps. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Some specification of encryption, but protocol not open source. Score 1	67
TELEGRAM	TELEGRAM MESSENGER	Yes, stated commitment to rights and recognition of online threats. Score 3	Has end-to-end encryption, but not set as a default. Score 1	Inadequate notification within the apps; no warning when using weaker encryption. Score 1	Commitment not to share user data, but no transparency report with details of requests received. Has taken public stance against encryption backdoors. Score 2	Yes, app is open source, although encryption implementation criticised. Score 3	67
GOOGLE	ALLO, DUO, HANGOUTS	Yes, but only committed to freedom of expression through participation in multi-stakeholder initiative. Score 2	Yes on Duo; but only as an option on Allo, Hangouts not at all. Score 1	Inadequate notification within the apps; no warning in Allo when using weaker encryption. Score 1	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	Allo uses open source Signal, but not published specification yet. Score 1	53
LINE	LINE	Commitment to rights, but no policy recognition of threats. Score 1	Yes. Score 3	Inadequate notification within the app. Score 1	No, does not publish transparency report. Has taken public stance against encryption backdoors. Score 1	Provides specification of encryption, but not open source protocol. Score 1	47
VIBER MEDIA	VIBER	No commitment to freedom of expression, no policy recognition of threats. Score 1	Yes. Score 3	Inadequate notification within the app. Score 1	No, does not publish transparency report. Has publicly rejected encryption backdoors. Score 1	Provides specification of encryption, but not open source protocol. Score 1	47
KAKAO INC	KAKAO TALK	Commitment to rights, but no policy recognition of threats. Score 1	Has end-to-end encryption, but not set as a default. Score 1	Inadequate notification within the apps; no warning when using weaker encryption. Score 1	Publishes transparency report. Has taken public stance against encryption backdoors. Score 3	Only basic information on system of encryption. Score 0	40
MICROSOFT	SKYPE	Yes, clear commitment to rights and recognition of online threats. Score 3	Skype does not have end-to-end encryption. Score 0	No information or warnings within app about level of encryption on Skype. Score 0	Yes, and notifies affected user unless legally prohibited. Has taken public stance against encryption backdoors. Score 3	No specification of Skype system of encryption. Score 0	40
SNAPCHAT	SNAPCHAT	No commitment to freedom of expression, no policy recognition of threats. Score 1	Snapchat does not have end-to-end encryption. Score 0	No information given to users on website or in app about level of encryption. Score 0	Yes, and notifies affected user. Refuses to backdoor encryption. Score 3	No specification of Snapchat system of encryption. Score 0	26
BLACKBERRY	BLACKBERRY MESSENGER	No commitment to freedom of expression, no policy recognition of threats. Score 1	No, only offers end-to-end encryption as separate paid service. Score 0	Explanation on website, but no reference to encryption within app itself. Score 1	No, does not publish transparency report. Has publicly rejected encryption backdoors, but alleged cases where not done so in practice. Score 0	Provides specification of encryption, but not open source protocol. Score 1	20
TENCENT	QQ, WECHAT	No recognition of threats, no commitment to freedom of expression. Score 0	WeChat not end-to-end encrypted, QQ encryption unclear. Score 0	No information given to users on website or in app about level of encryption. Score 0	No. Does not publish transparency report, does not publically refuse to backdoor encryption. Score 0	No specification about encryption. Score 0	0

Fonte: https://www.amnesty.org.nz/snapchat-skype-among-apps-not-protecting-users%E2%80%99-privacy.

Tuttavia, la situazione sembra essere sensibilmente migliorata negli ultimi anni grazie alla diffusione dei *transparency reports* analizzati nel paragrafo precedente, che costituiscono una prova evidente dello sforzo compiuto da diverse società per rendere il più trasparente possibile le procedure di raccolta ed utilizzo dei dati degli utenti, al fine di accrescere la fiducia di questi ultimi verso i soggetti di diritto privato.

4.1.4 L'ambito di applicazione della direttiva (UE) 680/2016: una lacuna nella tutela del singolo?

Un ulteriore aspetto problematico da evidenziare in questa sede concerne la cosiddetta *Law Enfocerment Directive*, effettiva dal 25 maggio 2018. La suddetta norma ha sollevato infatti diversi dubbi di natura interpretativa, in relazione soprattutto alla linea di demarcazione fra l'applicazione del regolamento e della direttiva. La direttiva si applica, in particolare, ai dati personali trattati dalle autorità competenti per scopi di prevenzione, indagine accertamento e perseguimento dei reati od esecuzione di sanzioni penali[449]. Si può pertanto ritenere che la direttiva costituisca *lex specialis* rispetto al regolamento, dal momento che essa viene applicata solo nei casi in cui i dati personali siano raccolti per le finalità appena descritte. Infatti, nel caso in cui le medesime autorità di *law enforcement* raccolgano e trattino i dati per scopi diversi da quelli indicati nella direttiva, troverà applicazione il regolamento (UE) 2016/679.
Orbene, a livello pratico un problema sorge tutte le volte in cui, ad esempio, i dati personali siano raccolti da società private, con riferimento ai quali trova quindi applicazione il regolamento (UE) 2016/679 e poi, però, successivamente trasmessi e trattati da autorità nazionali e di polizia, che dovranno, invece, conformarsi alla direttiva (UE) 2016/680. Sorge spontaneo domandarsi, in questi casi, fino a che punto del trattamento dei dati troverà applicazione il regolamento e quando inizierà, invece, ad applicarsi la direttiva. Occorre inoltre ricordare che nella disciplina in esame non è previsto alcun riferimento all'ipotesi in cui i dati utilizzati per ragioni di *law enforcement* siano raccolti da parti terze.

Invero, il rapporto fra regolamento (UE) 2016/679 e direttiva (UE) 2016/680 viene disciplinato solamente dai considerando 11 della direttiva e dal considerando 19 del regolamento. Nel primo caso viene stabilito che, qualora i dati siano raccolti da soggetti privati o pubblici ed utilizzati poi per finalità diverse da quelle di prevenzione, indagine ed

[449]Art. 2 direttiva (UE) 2016/680.

accertamento e perseguimento di reati, si applicherà con riferimento agli stessi il regolamento 679/2016[450]. Per contro, in base a quanto previsto dal considerando 19, viene in rilievo la direttiva nel caso in cui le autorità competenti ai sensi della direttiva (UE) 2016/680 siano chiamate a svolgere funzioni necessariamente volte al perseguimento di reati e all'esecuzioni di sanzioni penali[451]. In ogni caso, troverà applicazione la direttiva tutte le volte in cui le parti private raccolgano e trattino i dati personali per le finalità indicate dall'articolo 1, par. 1, della direttiva e/o per conto delle autorità di *law enforcement*[452]. In questi ultimi casi, in particolare, le autorità operano come titolari del trattamento e gli attori privati, invece, come responsabili del trattamento. Le ipotesi indicate devono essere sempre disciplinate "[…] da un contratto o un altro atto giuridico e dalle disposizioni applicabili ai responsabili del trattamento a norma della presente direttiva"[453].

Si può ritenere, pertanto, che mentre il regolamento (UE) 2016/679 si applica nella fase iniziale di raccolta dei dati, questi, se successivamente trattati per ragioni di *law enforcement*, dovranno essere disciplinati invece dalla direttiva (UE) 2016/680[454]. Come determinare, però, il momento esatto a partire dal quale troverà applicazione l'una o l'altra normativa? A riguardo, né il regolamento né la direttiva sembrano avere fornito una risposta esaustiva, per cui ancora sussiste, ad oggi, una area di intercettezza in cui di fatto potrebbero applicarsi, in maniera interscambiabile, sia l'una che l'altra fonte normativa.

La questione è di ampia rilevanza se si considera, inoltre, che le condizioni e le limitazioni per la raccolta e il trattamento dei dati personali per le finalità indicate nella direttiva sono meno restrittive, soprattutto sotto il profilo dei poteri in capo alle autorità di *law enforcement.* Le ragioni alla base di una minore tutela nei confronti dei singoli previsti nella direttiva, cui corrisponde un maggior margine di manovra da parte delle autorità statali, si rinvengono nella specifica funzione svolta dai dati sensibili in questo contesto e, in particolare, nella loro strumentalità ad identificare e perseguire gli autori dei reati,

[450]Considerando 11 direttiva (UE) 2016/680.
[451]Considerando 19 regolamento (UE) 2016/679.
[452]Un esempio di attori privati che agiscono, però, per conto della autorità di *law enforcement*, è rappresentato dai centri di analisi/laboratori che analizzano le prove raccolte in relazione ad una determinata fattispecie criminosa e i cui risultati vengono poi trasmetti alle autorità di polizia al fine di poter essere utilizzati nelle indagini preliminari o allegati agli atti del processo. Cfr. in dottrina N. PURTOVA, *Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships,* in *International Data Privacy Law* 2018, pag. 64.
[453]Considerando 11 direttiva (UE) 2016/680.
[454]Cfr. C. JASSERAND, *op. cit.,* v. sopra nota n. 284*,* pag. 158.

eseguire sanzioni penali, e nei diversi interessi in gioco che la normativa europea è chiamata a regolare e bilanciare. Invero, mentre il regolamento (UE) 679/2016 disciplina i rapporti tra le parti private o tra queste ultime e le autorità pubbliche, che non svolgono però funzioni di *law enforcement*, nella direttiva in esame, da un lato sussiste il bisogno di tutelare i diritti e le libertà degli individui e, dall'altro lato, quello di assicurare che le diverse finalità di natura pubblicistica siano realizzate anche attraverso il corretto funzionamento degli organi statali di polizia.

Queste diversità si proiettano, ad esempio, nella disciplina relativa al trattamento di dati sensibili. Con tale termine si indica l'insieme dei dati riferibili alle origini razziali, alle opinioni politiche e alle convinzioni religiose o dati genetici[455]. Invero, mentre in base all'articolo 9 del regolamento (UE) 2016/679 vige come regola generale il divieto di trattamento dei suddetti dati sensibili - salvo nei casi espressamente elencati nel secondo paragrafo della dettato normativo - nell'articolo 10 della direttiva un analogo divieto, invece, non sussiste. L'articolo stabilisce che i dati sensibili di un individuo possano essere trattati solo "[…] se strettamente necessario, soggetto a garanzie adeguate per i diritti e le libertà dell'interessato e soltanto: a) se autorizzato dal diritto dell'Unione o dello Stato membro; b) per salvaguardare un interesse vitale dell'interessato o di un'altra persona fisica; o c) se il suddetto trattamento riguarda dati resi manifestamente pubblici dall'interessato".

Inoltre, il diritto di accesso alle informazioni da parte dell'interessato, previsto all'articolo 13 della direttiva, risulta essere più limitato rispetto a quanto previsto dall'analogo articolo del regolamento. In base a quest'ultimo, infatti, l'interessato ha diritto a ricevere informazioni relative anche ad eventuali trasferimenti dei suoi dati personali verso un paese terzo o un'organizzazione internazionale o il merito ad una decisione di adeguatezza o meno da parte della Commissione. Questa possibilità non è, invece, prevista nel caso in cui i dati siano raccolti per finalità investigative, il perseguimento dei reati o per l'esecuzione di sanzioni penali. Inoltre, sempre in base a quanto previsto nella direttiva, le autorità di polizia possono ulteriormente limitare il diritto di accesso alle informazioni qualora ciò costituisca una misura necessaria e proporzionata in una società democratica, al

[455]Considerando 51 regolamento (UE) 2016/679.

fine di non compromettere le indagini investigative o per proteggere la sicurezza nazionale e i diritti e le libertà altrui[456].

Un'ulteriore differenza si rileva, infine, nelle condizioni che legittimano il trattamento dei dati personali nell'uno e nell'altro caso. Infatti, mentre nel caso di trattamento dei dati personali nell'ambito di applicazione del regolamento (UE) 2016/679 un ruolo primario viene giocato dal consenso dell'interessato, il quale costituisce una delle condizioni di liceità elencate dall'articolo 6 e soggetto, a sua volta, a specifici requisiti indicati all'articolo 7 - quali la riconducibilità del consenso all'interessato, il fatto che esso debba essere prestato in maniera libera, per iscritto e in maniera chiara ed inequivocabile, utilizzando un linguaggio chiaro e semplice – questo non è previsto, invece, nella direttiva.

Per quanto riguarda l'ambito di applicazione della direttiva (UE) 2016/680, un primo problema interpretativo si riscontra, ad esempio, nella mancanza di una chiara delimitazione di cosa esattamente rientri nelle attività di polizia e dell'utilizzo interscambiabile dei termini "pubblica sicurezza" e "ordine pubblico" da parte del legislatore europeo[457]. Si può dire, infatti, che la cosiddetta "Police Directive" sia stata quasi completamente oscurata dall'interesse esclusivo che ha suscitato, invece, il regolamento (UE) 2016/679, facente parte dello stesso "Pacchetto protezione dati" europeo, entrato in vigore il 25 maggio 2016 e divenuto appicabile in tutti gli Stati Membri dal 25 maggio 2018. Inoltre, occorre tenere in considerazione il crescente ruolo svolto dai soggetti di diritto privato nella raccolta e trattamento dei dati personali per finalità di *law enforcement* e sicurezza nazionale. Invero, il cosiddetto fenomeno PPP, che sta per "Public-private partnership", ha assunto negli ultimi anni una crescente importanza, evidenziata anche dal fatto che il Consiglio d'Europa abbia elencato il modello PPP tra quelli necessari per un nuovo approccio alla sicurezza informatica europea e che la nuova direttiva DIS[458] abbia stabilito come obbligatoria la stretta collaborazione tra i soggetti privati e quelli pubblici al fine di rinforzare la sicurezza informatica nazionale[459].

[456]Articolo 13, par. 3 direttiva (UE) 2016/680.
[457]Cfr. M. M. CARUANA, *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *International Review of Law, Computers & Technology 2017,* pag. 7
[458]Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio del 6 luglio 2016 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione.
[459]Cfr. N. PURTOVA, *op. cit.,* v. sopra nota 452, pag. 54.

Tradizionalmente, i soggetti di diritto privato possono collaborare in due modi alla attività di *law enforcement.* Tramite la prima modalità, che è sicuramente la più diffusa, le società restano al di fuori della struttura organizzativa delle entità preposte alle attività di *law enforcement* e non assumono, rispetto alle stesse, alcuno specifico *status.* In mancanza di ciò, risulta pertanto difficile identificare il diritto applicabile, e gli eventuali profili di responsabilità, nei confronti dei soggetti di diritto privato, i quali potrebbero assumere ciononostante anche ruoli decisivi nelle indagini e nell'identificazione degli autori dei reati, soprattutto di quelli commessi *online*[460].

La seconda modalità di collaborazione prevede, invece, un inglobamento effettivo dei soggetti privati nelle strutture organizzative di polizia, che può avvenire o attraverso la cosiddetta "sostituzione" dei civili, ossia quando agli stessi viene attribuito uno specifico ruolo nelle attività investigative – che può essere, ad esempio, quello di testimone o di collaboratore esterno, oppure attraverso la legalizzazione di attività compiute dai civili per contrastare la criminalità *online* (le cosiddette attività di vigilanza). Ci si domanda, quindi, se i soggetti di diritto privato possano essere considerati "autorità competenti" ai sensi della direttiva (UE) 680/2016, in base alla definizione delle stesse fornita dall'articolo 3, par. 1, punto 7. A riguardo sembra possibile fornire risposta affermativa, soprattutto alla luce di quanto previsto al punto 7 (b), ove i termini "qualsiasi altro organismo o entità incaricati dal diritto dello Stato membro di esercitare l'autorità pubblica" potrebbero includere anche società private[461]. In ogni caso, la mancanza di una chiara definizione di cosa esattamente si intenda per "autorità competente" è all'origine dei principali problemi di applicazione delle due normative e ciò impatta in maniera significativa anche sulle possibili imputazioni di responsabilità in caso di violazioni del diritto umano alla protezione dei dati personali.

Un altro problema interpretativo potrebbe inoltre sorgere inoltre con riferimento all'obbligo della specifica finalità del trattamento prevista all'articolo 5, par. 1 lett. b) regolamento (UE) 2016/679 e all'articolo 4, par. 1, lett. b della direttiva (UE) 2016/680. Invero i dati personali, raccolti per determinate finalità originarie, e riguardo alle quali il soggetto titolare aveva espresso il suo consenso, vengono poi successivamente trasmessi e trattati per delle finalità ulteriori e diverse, ossia quelle di indagine ed accertamento dei

[460] *Ibidem*, pag. 56.
[461] *Ibidem*, pag. 61.

reati indicate all'articolo 1 della direttiva. A ben vedere, però, il problema è solo apparente, nella misura in cui è lo stesso 23, par. 1 lett. d), regolamento (UE) 2016/679 a prevedere la possibilità di limitare gli obblighi e i diritti previsti dalla normativa europea qualora tale misura limitativa rispetti l'essenza dei diritti e delle libertà fondamentali e sia necessaria e proporzionata in una società democratica per "[…] la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, incluse la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica".

A livello pratico, nel caso in cui si constati una violazione del diritto alla protezione dei dati personali di un utente da parte di un'autorità di *law enforcement*, troverà sempre applicazione la direttiva (UE) 2016/680, essendo i dati raccolti e trasmessi per le finalità di cui all'articolo 1, par.1, e costituendo essi un'eccezione rispetto alle condizioni di liceità del trattamento previste dall'articolo 6 regolamento (UE) 2016/679, salvo i casi limite in cui, ad esempio, il mandato sia manifestamente illegittimo. Orbene, queste ultime fattispecie, in cui è possibile configurare una responsabilità anche in capo alla società per violazione del regolamento (UE) 2016/679, andranno risolte caso per caso, facendo anche ricorso ai tradizionali principi previsti dal diritto civile e penale dei diversi ordinamenti nazionali, quali potrebbero essere, per quanto per riguarda ad esempio l'ordinamento italiano, quello di correttezza e buona fede ai sensi degli articoli 1175[462] e 1337[463] c.c. e il limite dell'ordine manifestamente illegittimo ai sensi dell'articolo 51 c.p.[464].

[462]Articolo 1175 c.c. "Il debitore e il creditore devono comportarsi secondo le regole della correttezza".
[463]Articolo 1337 c.c. "Le parti, nello svolgimento delle trattative e nella formazione del contratto, devono comportarsi secondo buona fede".
[464]Articolo 51 c.p. "L'esercizio di un diritto o l'adempimento di un dovere imposto da una norma giuridica o da un ordine legittimo della pubblica autorità, esclude la punibilità. Se un fatto costituente reato è commesso per ordine dell'autorità, del reato risponde sempre il pubblico ufficiale che ha dato l'ordine. Risponde del reato altresì chi ha eseguito l'ordine, salvo che, per errore di fatto abbia ritenuto di obbedire a un ordine legittimo. Non è punibile chi esegue l'ordine illegittimo, quando la legge non gli consente alcun sindacato sulla legittimità dell'ordine".

4.1.5 Il crescente ruolo assunto dagli *Internet service provider* nella giurisprudenza della Corte di giustizia e della Corte europea dei diritti umani

Quale ulteriore evidenza dell'importanza assunta in questo contesto dalle società private vengono in rilievo, oltre ai recenti fatti esposti nell'introduzione del presente elaborato connessi alle rivelazioni di Snowden e ai programmi di sorveglianza di massa PRISM, anche le due sentenze della Corte di giustizia relative ai *Digital Rights Ireland Ltd* e *Tele2 Sverige AB*, analizzate nel precedente capitolo sotto altri profili problematici.

Entrambi i casi hanno infatti riguardato la raccolta dei dati da parte di operatori economici privati che esercitavano la propria attività nell'ambito dei servizi di comunicazione elettronica. I dati personali venivano poi trasmessi ed utilizzati alle autorità statali per finalità di *law enforcement* e per proteggere la sicurezza nazionale[465]. I giudici di Lussemburgo venivano pertanto chiamati a valutare se la cosiddetta *Data Retention Directive* in un caso, e la legge nazionale nell'altro caso, fossero compatibili con gli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea e se le misure di interferenza fossero giustificate ai sensi dell'articolo 52. "The assessment of the Court in the two cases is different: in *Digital Rights Ireland Ltd*, the Court analysed in details the different conditions under which derogations to the fundamental rights are permitted, whereas in *Tele2 Sverige*[466], the Court mainly focused on the proportionality of the national laws derogating the principle of confidentiality"[467]. La Corte di giustizia constatava ivi che entrambe le leggi non fossero conformi al principio di proporzionalità.

In questo contesto, una parte della dottrina ha evidenziato in maniera critica il fatto che, nonostante il caso *Digital Rights Ireland Ltd* fosse stato deciso quando la direttiva era ancora in fase di negoziazione – quindi soggetta a possibili modifiche - i principi sanciti dalla Corte di giustizia nel caso in esame, come ad esempio l'indicazione del numero di persone che potevano accedere ai dati personali o la previsione di una procedura di controllo preventivo[468] per le richieste di dati per ragioni di *law enforcement,* non fossero stati poi di fatto trasposti nella nuova normativa europea[469]. Pertanto, in mancanza di

[465]Cfr. C. JASSERAND, *op. cit.,* v. sopra nota 284, pag. 156.
[466]Corte di giustizia (Grande Sezione), *Tele2 Sverige AB*, cit., par. 95 e ss.
[467]Cfr. C. JASSERAND, *op. cit.,* v. sopra nota 284, pag. 160.
[468]Non è del tutto chiaro se la procedura di consultazione preventiva all'autorità di controllo prevista dall'articolo 28 direttiva (UE) 2016/680 possa di fatto considerarsi una procedura di revisione preventiva così come intesa nella sentenza *Digital Rights Irland Ltd*.
[469]*Ibidem*, pag. 161.

un'espressa indicazione nella direttiva in merito alla raccolta dei dati personali da parte delle società private, era stata avanzata l'ipotesi di inserire alcuni articoli in materia nella proposta di regolamento *e-privacy*, seppur limitatamente ai soli dati raccolti elettronicamente in ragione dell'ambito di applicazione materiale della normativa[470]. Tuttavia, nell'ultima versione della proposta pubblicata a gennaio 2017 non viene fatto alcun riferimento al trattamento da parte di soggetti di diritto privato.

Per quanto concerne, invece, la giurisprudenza della Corte europea dei diritti umani, non vi sono ad oggi pronunce in materia di misure di interferenza nel diritto alla privacy da parte di società private, essendo i ricorsi individuali limitati, in base a quanto previsto dall'articolo 34 CEDU, alle violazioni poste in essere dagli Stati membri. Tuttavia, i giudici di Strasburgo non si mostrano del tutto indifferenti al problema. Al riguardo viene in rilievo infatti l'opinione concorrente del giudice spagnolo relativa al caso *Szabó e Vissy c. Ungheria*, ove egli afferma che "In May 2015 the Council of Europe Commissioner for Human Rights published an issue paper on «Democratic and effective oversight of national security services», advocating that independent ex ante authorization should be extended to untargeted bulk collection of information, the collection of and access to communications data, *including when held by the private sector*, and, potentially, computer network exploitation. The process by which intrusive measures are authorized or re-authorized should itself be subject to scrutiny. States must ensure that individuals can also access a supervisory institution equipped to make legally binding orders"[471].
Inoltre, nonostante la stessa Corte abbia più volte tenuto a precisare che non sia sua competenza giudicare le violazioni dei diritti umani poste in essere da società private, negli ultimi anni essa ha dimostrato una maggiore apertura a far rientrare le suddette ipotesi in violazioni dell'articolo 8 CEDU, in ragione degli obblighi positivi gravanti sugli Stati in base alla suddetta norma.

In particolare, nel recente caso *López Ribalda e altri c. Spagna*, relativo a misure di video sorveglianza poste in essere dal datore di lavoro nei confronti dei propri dipendenti, la Corte europea dei diritti umani affermava che: "[…] although the purpose of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this

[470] *Ibidem*, pag. 165.
[471] Corte europea dei diritti umani, *Szabó e Vissy c. Ungheria*, Opinione concorrente del giudice Pinto De Albuquerque, par. 12.

primarily negative undertaking, there may be positive obligations inherent in an effective respect for private life"[472].

Questa soluzione, praticata al momento solo con riferimento alle violazioni del diritto alla privacy sul luogo del lavoro o alla violazione dell'articolo 8 CEDU sotto il profilo della tutela ambientale e del rispetto alla vita privata e familiare, potrebbe essere eventualmente estesa anche ai casi in cui le società e *gli Internet service provider* trasmettano ingiustificatamente i dati alle autorità di *law enforcement* al fine di sorvegliare, anche in maniera indiscriminata, gli individui.

4.2 L'ESERCIZIO EXTRATERRITORIALE DELLA GIURISDIZIONE E LA TUTELA DEI DIRITTI UMANI

Prima di procedere all'analisi delle problematiche connesse alla violazione dei dati personali e all'eventuale applicazione extraterritoriale dei trattati internazionali e regionali che li tutelano, si rende opportuno procedere ad un'analisi più generale dei diversi casi finora trattati dagli organi internazionali di controllo in materia di esercizio extraterritoriale della giurisdizione.

Dal punto di vista metodologico, quest'analisi permette infatti di fornire le basi per valutare un'eventuale applicazione analogica dei principi, sanciti principalmente dalla Commissione Interamericana dei diritti umani e dalla Corte europea dei diritti umani, anche ai casi di violazione del diritto alla protezione dei dati personali, su cui nessun tribunale ad oggi si è ancora pronunciato. Invero, in mancanza di un sistema normativo e giurisprudenziale adeguato in materia, una delle soluzioni più praticabili sembra essere il ricorso al metodo dell'analogia per provare a colmare le lacune.

Inoltre, come si avrà modo di vedere più avanti, un segnale senz'altro positivo verso una maggiore applicazione extraterritoriale della tutela dei dati personali è stato dato dal nuovo 3 regolamento (UE) 2016/679, che costituisce espressione del principio di territorialità e degli effetti.

[472]Corte europea dei diritti umani, *López Ribalda e altri c. Spagna*, sentenza del 9 gennaio 2018, ricorsi nn. 1874/13 e 8567/13, par. 60. In maniera analoga si è pronunciata la Grande Camera nel caso *Barbulescu c. Romania*, sentenza del 5 settembre 2017, ricorso n. 61496/08, par. 108.

L'utilizzo massiccio degli strumenti tecnologi di comunicazione solleva numerosi problemi di difficile risoluzione, in parte già analizzati nel capitoli precedenti, cui si aggiunge anche quello relativo alla possibilità per la Corte europea dei diritti umani di esercitare la giurisdizione con riferimento alle violazioni poste in essere al di fuori del territorio di competenza. Invero, secondo quando stabilito dall'articolo 56 CEDU "Ogni Stato, al momento della ratifica o in ogni altro momento successivo, può dichiarare, mediante notifica indirizzata al Segretario generale del Consiglio d'Europa, che la presente Convenzione si applicherà, con riserva del paragrafo 4 del presente articolo, su tutti i territori o su determinati territori su esso cura le relazioni internazionali". In conseguenza di ciò, i giudici di Strasburgo possono esaminare i casi di violazioni ai sensi degli articoli 33[473] e 34[474] da parte degli Stati contraenti, anche qualora queste siano commesse oltre i confini territoriali attraverso atti direttamente riconducibili alle autorità statali. In base alla dottrina internazionale "the extraterritoriality or extraterritorial application of international and European human rights treaties refers to the recognition by those treaties' states parties of the international and European human rights of individuals or groups of individuals situated outside their territory and, in a second stage, to the identification of their corresponding duties to those individuals"[475].

Il problema dell'applicazione extraterritoriale dei trattati che tutelano i diritti umani non è noto solo alla Corte europea dei diritti umani, potendosi rinvenire diversi casi anche nel sistema interamericano, più risalenti nel tempo, ma di sicuro rilievo[476]. L'articolo 1 della Convenzione americana sui diritti umani[477] stabilisce infatti che "Gli Stati Parte della Convezione si impegnano a rispettare i diritti e le libertà da essa riconosciuti e ad assicurare a tutte le persone soggette alla loro giurisdizione il libero e pieno esercizio di tali

[473]Articolo 33 CEDU "Ogni Alta Parte contraente può deferire alla Corte qualunque inosservanza delle disposizioni della Convenzione e dei suoi Protocolli che essa ritenga possa essere imputata a un'altra Alta Parte contraente".

[474]Articolo 34 CEDU "La Corte può essere investita di un ricorso da parte di una persona fisica, un'organizzazione non governativa o un gruppo di privati che sostenga d'essere vittima di una violazione da parte di una delle Alte Parti contraenti dei diritti riconosciuti nella Convenzione o nei suoi protocolli. Le Alte Parti contraenti si impegnano a non ostacolare con alcuna misura l'esercizio effettivo di tale diritto".

[475]S. BESSON, *The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amount to,* in *Leiden Journal of International Law* 2012, pag. 858. Sul tema cfr. anche M. MILANOVIC, *Extraterritorial application of human rights treaties: Law, principles and policy,* Oxford University Press 2011.

[476]Cfr. C. M. CERNA, *Extraterritorial Application of the Human Rights Instruments of the Inter-American System*, in F. COOMANS, M.T. KAMMINGA, *Extraterritorial application of human rights treaties*, Intersentia 2004, page 105 ss.

[477]Convenzione americana sui diritti umani, adottata dall'Organizzazione degli Stati Americani (OAS) il 21 novembre 1969 a San José di Costarica ed entrata in vigore il 18 luglio 1978.

diritti e libertà, senza alcuna discriminazione per ragioni di razza, colore, sesso, lingua, religione, opinioni politiche o di qualsiasi altra natura, origine nazionale o sociale, condizione economica, nascita o altra condizione sociale". Il criterio territoriale enunciato nella norma in esame presenta però diverse eccezioni, tra cui quella, comune al sistema CEDU, delle operazioni militari all'estero e delle violazioni dei diritti umani sulla base del criterio del "controllo effettivo".

La Commissione interamericana dei diritti umani si è sempre mostrata piuttosto aperta verso l'applicazione extraterritoriale della Convenzione. Ad esempio, nel caso *Victor Saldaño c. Argentina* del 1999[478], relativo ad un ricorso presentato da un cittadino argentino per essere stato condannato a morte negli Stati uniti e con il quale chiedeva al governo argentino di presentare un ricorso interstatale agli Stati Uniti, la Commissione interamericana dei diritti umani affermava che il termine "giurisdizione" contenuto nell'articolo 1 della Convenzione americana sui diritti umani non fosse da intendersi come strettamente collegato al territorio nazionale e che, conseguentemente, uno stato contraente potesse essere considerato responsabile anche per le azioni ed omissioni compiute dai suoi agenti al di fuori del territorio dello Stato.

Per quanto riguarda, invece, l'applicazione extraterritoriale della Dichiarazione americana dei diritti e dei doveri dell'uomo[479], i due principali casi hanno riguardano l'intervento dell'esercito statunitense a Grenada nel 1983 e a Panama nel 1989. Con riferimento al primo intervento militare, venivano presentati due ricorsi, uno relativo al bombardamento di un manicomio in cui erano rimaste uccise sedici persone e poi risolto in maniera amichevole, l'altro relativo invece ad alcune persone coinvolte in azioni di sovvertimento al governo. Nel 1983, infatti, le forze militari degli Stati Uniti e dei Caraibi invadevano Grenada e deponevano il governo rivoluzionario. Durante l'occupazione militare alcune delle persone coinvolte nei movimenti rivoluzionari venivano arrestate e detenute dalle forze statunitensi. Diciassette persone presentarono una petizione di fronte alla Commissione americana in ragione della detenzione. La Commissione interamericana dei diritti umani affermava ivi che la Dichiarazione americana dei diritti e dei doveri dell'uomo dovesse essere intesa come una fonte di obblighi anche per gli Stati terzi.

[478]Commissione interamericana dei diritti umani, *Petition Victor Saldaño c. Argentina*, 11 marzo 1999, Rapporto n. 38/99.

[479]Dichiarazione americana dei diritti e dei doveri dell'uomo, adottata dall'Organizzazione degli Stati americani durante la IX Conferenza Internazionale a Bogotá, Colombia, nel 1948.

Inoltre, "were the Commission to decline to exercise jurisdiction in such a case, it would risk leaving fundamental rights unprotected, in contravention of the mandate which it is in charged"[480].

Il secondo caso riguardava, invece, il ricorso presentato in seguito alle operazioni militari da parte delle truppe statuniteni a Panama nel 1989[481]. I ricorrenti lamentavano che le truppe USA avessero agito senza considerare la sicurezza dei cittadini di Panama durante le operazioni militari nel paese, in violazione dei diritti sanciti nella Dichiarazione dei diritti e dei doveri dell'uomo. La Commissione interamericana dei diritti umani riteneva di avere competenza per decidere tutte le violazioni dei diritti umani, avendo questi ultimi assunto ormai valore di *ius cogens*. Infine, un altro caso degno di menzione è quello relativo all'intervento militare dell'esercito cubano nel 1994[482], che aveva abbattuto diversi aerei civili su cui erano a bordo dei cittadini americani. Ivi la Commissione interamericana dei diritti umani aveva ritenuto di essere competente a giudicare le violazioni dei diritti umani compiuti da Stati membri dello OAS anche al di fuori del territorio dello Stato, dal momento che l'extraterritorialità non faceva venire meno l'obbligo per gli Stati di rispettare i diritti sanciti nella Dichiarazione .

Si può ritenere, pertanto, che nel sistema di tutela interamericano l'esercizio extraterritoriale della giurisdizione si giustifichi principalmente sulla base del controllo effettivo, sul territorio o sulle persone. In una recente Opinione consultiva, però, datata al 15 novembre 2017[483], la Corte interamericana dei diritti umani parrebbe avere introdotto un terzo criterio di attribuzione della giurisdizione, basato sulla conoscenza da parte dello Stato dei rischi connessi ad una certa attività e sulla capacità di controllarla e prevenire eventuali danni. Anche la Corte europea dei diritti umani aveva, in realtà, già avanzato l'ipotesi del criterio degli effetti nel *caso Al-Skeini e altri c. Regno Unito*, ma in maniera sempre molto vaga e senza alcuna applicazione concreta:"[…] acts of the Contracting

[480]Commissione interamericana dei diritti umani, *Coard Et Al. c. Stati Uniti*, 29 settembre 1999, Rapporto n. 109/99, par. 43.
[481]Commissione interamericana dei diritti umani, *Case 10.573 c. Stati Uniti*, 14 ottobre 1993, Rapporto n. 31/93.
[482]Commissione interamericana dei diritti umani, *Case 11.589 Armando Alejandre Jr., Carlos Costa, Mario De La Peña, And Pablo Morales c. Cuba*, 29 settembre 1999, Rapporto n. 86/99.
[483]Corte interamericana dei diritti umani, *Solicitada por la Republica de Colombia Medio Ambiente y Derechos Humanos*, 15 novembre 2017, Opinione Consultiva Oc-23/17.

States […] **producing effects** outside their territories can constitute an exercise of jurisdiction within the meaning of Article 1"[484].

Orbene, pur riconoscendo gli effetti positivi che l'opinione della Corte interamericana dei diritti umani potrebbe apportare in termini di maggiore tutela dei diritti umani, sono stati resi evidenti alcuni aspetti critici di essa, legati soprattutto alla mancata indicazione della soglia di gravità delle violazioni oltre la quale può essere riconosciuto l'esercizio della giurisdizione, e la sua estensione o meno a tutti i diritti tutelati dalla Convenzione interamericana.

Un tema strettamente connesso all'esercizio extraterritoriale della giurisdizione in materia di tutela dei diritti umani è quello dell'universalità della giurisdizione[485]. In base al suddetto criterio "[….] certain crimes are so heinous, and so universally recognized and abhorred, that a state is entitled or even obliged to undertake legal proceedings without regard to where the crime was committed or the nationality of the perpetrators or the victims"[486]. Il dibattito in merito all'eventuale previsione di una giurisdizione universale, invocabile soprattutto in relazione ai più gravi crimini internazionali[487], sembra essersi al momento arrestato, presa forse anche coscienza degli insormontabili limiti che persistono in ragione delle peculiarità proprie dei diversi sistemi giurisdizionali e legislativi nazionali, su cui gli Stati sovrani non sono disposti a cedere, e che di fatto rendono quello dell'universalità della giurisdizione un argomento forse più ipotetico, strettamente dottrinale, che concretamente applicabile. Inoltre, secondo quanto sostenuto da parte della dottrina, affermare il principio della giurisdizione universale in materia di diritti umani non solo non sarebbe risolutivo in termini di una più effettiva tutela, ma risulterebbe anche erroneo dal punto di vista normativo in quanto "[…] contradicts the way in which international human rights treaties only apply formally to every given state party's

[484]Corte europea dei diritti umani (GC), *Al-Skeini And Others V. The United Kingdom*, sentenza del 7 luglio 2011, ricorso n. 55721/07, par. 131.
[485]In dottrina cfr. P. MAGNARELLA, *Universal Jurisdiction and Universal Human Rights: A Global Progression*, in *Journal of Third World Studies*, 1995; C. RYNGAERT, *Universal Jurisdiction over International Crimes and Gross Human Rights Violations: The Role of the Principle of Subsidiarity*, Oxford University Press 2016.
[486]S. MACEDO, *Universal Jurisdiction, National Courts and the Prosecution of Serious Crimes under International Law,* University of Pennsylvania Press 2004, pag. 4. Cfr. anche L. REYDAMS, *Universal Jurisdiction*, Oxford Monographs in International Law, Oxford, 2004; S. ZAPPALA', *L'universalità della giurisdizione e la Corte penale Internazionale*, *in Problemi attuali della giustizia penale internazionale*, il Mulino, Bologna 2005.
[487]Cfr. D. IRELAND-PIPER, *Accountability in Extraterritoriality, A comparative and International Law perspective*, Edward Elgar Publishing, 2017, pag. 29.

institutions and not to all other states at once, and not to other subjects of international law but to states, on the one hand, and only vis-a`-vis certain individuals situated in a specific relationship to them and not to everyone, on the other"[488].

In ogni caso, per ragioni connesse all'oggetto di indagine, non è possibile in questa sede approfondire ulteriormente il lungo dibattito sorto in merito al principio della giurisdizione universale. Ci si limiterà ad evidenziare come, nonostante il dibattito in materia si sia al momento arrestato, resti tuttora irrisolta la questione di come conciliare il carattere transfrontaliero di Internet, luogo in cui avvengono al giorno d'oggi il maggior numero di scambi di dati personali, con quello, invece, territorialmente limitato e tipico degli organi giurisdizionali e delle fonti normative preposte a tutelare gli individui nei confronti dell'illecito utilizzo e trasmissione dei suddetti dati.

4.2.1 L'esercizio extraterritoriale della giurisdizione in caso di esercizio della facoltà di deroga prevista dal Patto sui diritti civili e politici e dalla CEDU

Nei prossimi paragrafi verranno analizzati alcuni aspetti problematici legati, soprattutto, all'esercizio extraterritoriale della giurisdizione della Corte europea dei diritti umani in caso di deroghe *ex* articolo 15 CEDU, e all'eventuale applicazione dei principi del controllo effettivo e degli effetti anche in materia di tutela internazionale dei dati personali. In particolare, si è deciso di porre l'attenzione solo sui casi di applicazione extraterritoriale della CEDU in caso di esercizio della facoltà di deroga per ragioni di emergenza nazionale, perché è ivi che sono stati enunciati i principi del controllo effettivo e degli effetti, eventualmente invocabili anche in materia di tutela dei personali. Le altre due eccezioni al principio di territorialità riguardano, invece, i casi di estradizione o espulsione e i casi di protezione diplomatica o consolare[489].

Orbene, uno dei temi maggiormente dibattuti in dottrina e giurisprudenza ha riguardato proprio l'applicazione extraterritoriale dei trattati internazionali sui diritti umani anche durante i conflitti armati e le occupazioni militari sui territori stranieri[490]. In questo

[488]S. BESSON, *op. cit.,* v. sopra nota 475, pag. 859.
[489]Cfr. S. MILLER, *Revisiting Extraterritorial Jurisdicition: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention,* in *The European Journal of International Law* 2010*,* pag. 1227.
[490]Cfr. S.R. RATNER, *Human Rights for Whom?: Territoriality, Extraterritoriality, and Universal Jurisdiction*, in *The Thin Justice of International Law*, Oxford University Press 2015, pag. 268.

contesto, infatti, si poneva originariamente il problema dell'eventuale contrasto tra il diritto umanitario, tradizionalmente applicato durante i conflitti armati, e il sistema internazionale di tutela dei diritti umani, che trovava applicazione, invece, solo in tempi di pace. Nel corso degli anni questo contrasto è andato via via appianandosi, fino ad essere superato da una parte consistente della dottrina, la quale ha ritenuto che l'applicazione del diritto umanitario non fosse di per sé motivo di esonero per gli Stati del loro obbligo di rispettare i trattati internazionali sui diritti umani. Ad esempio, nel 2004 la Corte internazionale di giustizia, chiamata a pronunciarsi con un parere in merito alla costruzione di un muro sui territori occupati palestinesi, ha ritenuto applicabili in questo contesto sia il Patto Internazionale sui diritti civili e politici che la Convenzione sui diritti del fanciullo e che, allo stesso tempo, la costruzione di barriere di sicurezza come il muro costituisse una violazione del diritto umanitario[491].

Per quanto riguarda invece il sistema di tutela previsto dalla CEDU, la Corte europea dei diritti umani si è pronunciata in Grande Camera nel 2001 nel caso *Bankovic c. Belgio*[492]*,* avente ad oggetto il bombardamento di alcuni edifici appartenenti alla Radio Televisione Serba da parte delle forze militari della NATO. La questione riguardava, in particolare, la possibilità per le vittime di atti compiuti extra territorialmente di cadere sotto la giurisdizione degli Stati contraenti[493]. In questo caso, i giudici di Strasburgo escludevano che le vittime potessero considerarsi soggetti alla giurisdizione degli Stati contraenti ai sensi dell'articolo 1 CEDU, anche alla luce dell'interpretazione restrittiva fornita alla norma dai *travaux préparatoires* dell'Assemblea Parlamentare del Consiglio d'Europa e dal fatto che "[…] no State has indicated a belief that its extra-territorial actions involved an exercise of jurisdiction within the meaning of Article 1 of the Convention by

[491]Corte internazionale di giustizia, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Parere consultivo, 9 luglio 2004, general list no. 131.

[492]Corte europea dei diritti umani (GC), *Bankovic e altri c. Belgio*, sentenza del 12 dicembre 2001, ricorso n. 52207/99. Sull'applicazione extraterritoriale della CEDU cfr. i seguenti casi della Corte europea dei diritti umani: *Pisari c. Repubblica di Moldavia e Russia,* sentenza del 21 aprile 2015, ricorso n. 42139/12; (GC) *Hassan c. Regno Unito,* sentenza del 16 settembre 2014*,* ricorso n. 29750/09*;* (GC) *L-Skeini e altri c. Regno Unito*, cit.; *Manitaras e altri c. Turchia,* sentenza del 3 giugno 2008, ricorso n. 54591/00; *Pad e altri c. Turchia*, sentenza del 28 giugno 2007, ricorso n. 60167/00; *Behrami e Behrami c. Francia,* sentenza del 31 maggio 2007, ricorso n. 71412/01; (GC) *Markovic e altri c. Italia*, sentenza del 14 dicembre 2006, ricorso n. 1398/03; *Saddam Hussein c. Albania, Bulgaria, Croatia, Repubblica Ceca, Danimarca, Estonia, Ungheria, Islanda, Irlanda, Italia, Lituania, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Turchia, Ukraina e Regno Unito,* sentenza del 14 marzo 2006, ricorso n. 23276/04; (GC) *Cipro c. Turchia,* sentenza del 10 maggio 2001, ricorso n. 25781/94.

[493]In dottrina cfr. S. BESSON, *op. cit.*, v. sopra nota 475, pagg. 857-884; V. MANTOUVALOU, *Extending Judicial Control in International Law: Human Rights Treaties and Extraterritoriality*, in *The International Journal of Human* Rights 2011, pagg. 147-163.

making a derogation pursuant to article 15 of the Convention […]"[494]. Inoltre, prosegue la sentenza, "[…] the Court does not find any basis upon which to accept the applicant's suggestion that Article 15 covers all "war" and "public emergency" situations generally, whether obtaining inside or outside the territory of the Contracting State. Indeed, Article 15 itself is to be read subject to the "jurisdiction" limitation enumerated in Article 1 of the Convention"[495]. Sempre sulla base del controllo effettivo i giudici di Strasburgo giungevano nel caso *Al-Skeini & altri c. Segretario di Stato per la difesa*[496] alla conclusione che "[…] since the death occurred in the course of a United Kingdom security operation, when British soldiers carried out a patrol in the vicinity of the applicant's home and joined in the fatal exchange of fire, there was a jurisdictional link between the United Kingdom and this deceased also"[497].

In relazione a questi casi è stato inoltre constatato come, nonostante numerosi Stati abbiano effettuato diverse missioni militari all'estero fin dall'entrata in vigore della CEDU, nessuno di questi abbia mai specificato, nell'invocare l'esercizio della facoltà di deroga ai sensi dell'articolo 15, che le attività condotte all'estero potessero costituire esercizio della giurisdizione statale[498].
Conseguentemente, nel sistema CEDU l'esercizio extraterritoriale della giurisdizione da parte della Corte deve considerarsi del tutto eccezionale, potendo essa essere invocata solo nelle quattro diverse ipotesi enunciate nella sentenza *Bankovic*, tra cui assume particolare rilievo il caso in cui uno Stato membro della Convenzione, attraverso il controllo effettivo su certi territori e sulla loro popolazione, in seguito ad un'occupazione militare o tramite il consenso dello Stato occupato, eserciti i poteri pubblici propri di questi ultimi.

Per quanto riguarda, invece, il sistema di tutela previsto dal Patto sui diritti civili e politici, non si riscontra alcuna prassi in merito ad un'eventuale applicazione extraterritoriale del trattato, dal momento che tutte le deroghe invocate ai sensi dell'articolo 4 hanno sempre riguardato situazioni di emergenza interne allo Stato. Ciononostante, nel 2004 il Comitato per i diritti umani si è espresso con il *General*

[494]Corte europea dei diritti umani (GC), *Bankovic e altri c. Belgio,* cit. par. 62.
[495]*Ibidem*, par. 62.
[496]Corte europea dei diritti umani (GC), *AL-Skeini e altri c. Regno Unito*, cit., par. 116.
[497]*Ibidem*, par. 150.
[498]Cfr. M. DENNIS, *Application of Human Rights Treaties Extraterritoriality During Times of Armed Conflict and Military Occupation,* in *Proceedings of the Annual Meeting (American Society of International Law),* Vol. 100, 2006, pag. 88.

Comment n. 31 in merito all'interpretazione da fornire all'articolo 2, par. 1[499], ove viene stabilito che l'applicazione del Patto non è limitata ai cittadini degli Stati firmatari, bensì si estende a tutti gli individui "[…] regardless of nationality or statelessness, such as asylum seekers, refugees, migrant workers and other persons, who may find themselves in the territory or subject to the jurisdiction of the State Party […]"[500].

Pertanto, il trattato internazionale trova applicazione anche nei confronti delle persone soggette al potere o all'effettivo controllo di forze militari di uno Stato membro, che svolgono attività al di fuori del territorio nazionale, a prescindere dal modo in cui il controllo era stato ottenuto e dal fatto che si trattasse di operazioni di *peace-keeping* o *peace-enforcement.*

Tuttavia, malgrado l'interpretazione estensiva fornita alla norma dal Comitato per i diritti umani, resta tuttora il problema della formulazione letterale dell'articolo 2, che parla espressamente di "within its territority", enunciazione del criterio della territorialità giurisdizionale, e non, invece, di "within its jurisdiction", così com'era previsto nella formulazione originaria della norma, che lasciava intendere una maggiore apertura verso l'esercizio universale della giurisdizione. L'attuale enunciazione dell'articolo 2 costituisce, infatti, il frutto di un'esplicita richiesta di emendamento avanzata dagli Stati Uniti durante i lavori preparatori, intimoriti che l'espressione "within its jurisdiction" potesse comportare eccessivi obblighi di tutela dei diritti umani a carico degli Stati membri con riguardo, soprattutto, ai cosiddetti territori dati in concessione internazionale[501].

In conclusione, si può ritenere che l'applicazione extraterritoriale dei trattati internazionali sui diritti umani si basi ancora oggi principalmente sul criterio del controllo, o sul territorio o sulle persone, cui parte della dottrina sembra avere recentemente aggiunto anche un terzo criterio, basato sul controllo dei dati personali. Quest'ultimo, se praticato,

[499]Articolo 2, par. 1, Patto internazionale sui diritti civili e politici "Ciascuno degli Stati parti del presente Patto si impegna a rispettare ed a garantire a tutti gli individui che si trovino sul suo territorio e siano sottoposti alla sua giurisdizione i diritti riconosciuti nel presente Patto, senza distinzione alcuna, sia essa fondata sulla razza, il colore, il sesso, la lingua, la religione, l'opinione politica o qualsiasi altra opinione, l'origine nazionale o sociale, la condizione economica, la nascita o qualsiasi altra condizione".

[500]Comitato per i diritti umani, *General Comment no. 31*, *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 26 maggio, CCPR/C/21/Rev.1/Add. 1326, par. 10.

[501]Nel diritto internazionale, la Concessione internazionale un fenomeno tramite cui uno Stato dà in appunto in concessione, solitamente per finalità di natura economica, l'esercizio dell'autorità di governo ad uno Stato straniero, conservando sul territorio nazionale la propria sovranità. Per un maggiore approfondimento sulla tematica cfr., ad esempio, M. J. STRAUSS, *Territorial Leasing in Diplomacy and International Law*, Brill Nijhoff, Leida 2005.

sposterebbe di fatto l'esercizio del controllo effettivo dal piano strettamente materiale ad uno quasi completamente virtuale[502].

4.2.2 L'applicazione extraterritoriale del regolamento (UE) 2016/679 e la compatibilità con i principi sanciti dal diritto internazionale consuetudinario

"Il progressivo sviluppo di Internet e delle nuove tecnologie dell'informazione e di comunicazione hanno determinato la creazione di un dominio nuovo rispetto a quelli "tradizionalmente" conosciuti ed esplorati dall'uomo. Si tratta del cosiddetto «spazio cibernetico» nell'ambito del quale si originano, svolgono ed esauriscono differenti attività umane[503]". La natura stessa del ciberspazio, che si caratterizza per la mancanza di una specifica territorialità, da adito a diversi problemi legati, soprattutto, all'identificazione del luogo esatto in cui in cui il fatto illecito, i cui effetti spesso si sono però prodotti oltre i confini di un certo Stato, si è originato. Invero, l'identificazione del suddetto luogo permetterebbe di attribuire la responsabilità ad un certo Stato, e conseguentemente a chiedere il risarcimento qualora da una certa attività ne sia derivato un danno, quantificabile in anche termini economici.

Al riguardo, un chiaro segnalo verso una maggiore estensione della tutela dei dati personali è stato dato dal nuovo regolamento (UE) 2016/679, che si pone l'ambizioso obiettivo di avere applicazione extraterritoriale, dal momento che, in base a quanto previsto all'articolo 3, esso "[…] si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, *indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione*". La presenza di un titolare o responsabile del trattamento all'interno dell'Unione non è di per sé sufficiente a rendere applicabile la normativa europea, ma è necessario che i dati vengano trattati nell'ambito delle attività di uno stabilimento dell'Unione[504].

---

[502]Cfr. M. TAYLOR, *Transatlantic Juridictional Conflicts in Data Protection Law, How the Fundamental Right to Data Protection Conditions the European Union's Exercise of Extraterritorial Jurisdiction,* GVO drukkers & vormgevers 2018, pag. 52.

[503]M. BONFANTI, *Cyber-security e privacy: la promozione della sicurezza nello spazio cibernetico attraverso la tute-la della vita privata e la protezione dei dati personali* in U. Gori S. Lisi (a cura di), *Information warfare 2015 Manovre cibernetiche: impatto sulla sicurezza nazionale*, Milano, 2016, pag. 205.

[504]Per un'analisi più dettagliata di cosa si intenda per "ambito delle attività di uno stabilimento" confronta la sentenza della Corte di giustizia (Grande Sezione), *Google Spain SL Agencia Española de Protección de*

Al secondo comma è prevista un'ulteriore ipotesi di applicazione extraterritoriale della normativa europea, ossia con riguardo al trattamento dei dati personali di interessati che si trovano nell'Unione, ma effettuato da un titolare del trattamento o da un responsabile del trattamento non stabiliti nell'Unione, quando le attività di trattamento riguardano l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, oppure il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione.

Infine, l'articolo 3 prevede all'ultimo comma un'ulteriore ipotesi di applicazione extraterritoriale qualora il trattamento sia effettuato da un titolare del trattamento non stabilito nel territorio nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico[505].

Occorre sottolineare inoltre, che, pur facente parte dello stesso "Pacchetto protezione dati", un'analoga disposizione non è prevista invece nella direttiva (UE) 680/16 relativa alla raccolta e al trattamento dei dati personali per finalità di indagine e accertamento dei reati. La mancata estensione extraterritoriale della direttiva sarebbe dovuta al principio quasi esclusivamente territoriale che continua a regolare i sistemi penali nazionali.

L'estesa, e forse per alcuni "aggressiva"[506], applicazione extraterritoriale del regolamento (UE) 2016/679 si giustificherebbe in ragione dell'obbligo incombente sull'Unione europea di proteggere il diritto alla protezione dei dati sancito dall'articolo 8 della Carta dei diritti fondamentali dell'Unione europea, unitamente alla circostanza per cui quest'ultima è soggetta, in base a quanto previsto dagli articoli 3, par. 5[507], e 21, par.

Datos, Mario Costeja González, 13 maggio 2014, C- 131/12. In particolare, ivi viene stabilito che l'ambito delle attività di uno stabilimento viene in essere tutte le volte in cui "the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State".

[505]In realtà, già nella precedente direttiva 95/46/CE era prevista all'articolo 4, par. 1 lett. c), un'ipotesi di applicazione extraterritoriale della normativa europea nei casi in cui "il responsabile, non stabilito nel territorio della Comunità, ricorre, ai fini del trattamento di dati personali, a strumenti, automatizzati o non automatizzati, situati nel territorio di detto Stato membro, a meno che questi non siano utilizzati ai soli fini di transito nel territorio della Comunità europea".

[506]M. TAYLOR, *The EU's human rights obligations in relation to its data protection law with its extraterritorial effect,* in *International Data Privacy Law* 2015, pag. 256.

[507]Articolo 3, par. 5, TUE "Nelle relazioni con il resto del mondo l'Unione afferma e promuove i suoi valori e interessi, contribuendo alla protezione dei suoi cittadini. Contribuisce alla pace, alla sicurezza, allo sviluppo sostenibile della Terra, alla solidarietà e al rispetto reciproco tra i popoli, al commercio libero ed equo, all'eliminazione della povertà e alla tutela dei diritti umani, in particolare dei diritti del minore, e alla rigorosa osservanza e allo sviluppo del diritto internazionale, in particolare al rispetto dei principi della Carta delle Nazioni Unite".

1[508], TUE, alle norme di diritto internazionale pubblico e si impegna a rispettare i principi sanciti nella Carta delle Nazioni Unite e a promuovere i diritti umani. A livello giurisprudenziale, la Corte di Lussemburgo ha inoltre specificato nel caso *Air Transport Association of America*[509] che "[…] l'Unione è tenuta a rispettare il diritto internazionale nella sua globalità, ivi compreso il diritto internazionale consuetudinario al cui rispetto sono vincolate le istituzioni dell'Unione medesima"[510].
Tutto ciò porta all'ulteriore conseguenza che, anche in materia di tutela dei dati personali, potrà essere fatto ricorso ai principi sanciti dal diritto internazionale pubblico in tema di giurisdizione[511]. In realtà, già in passato la Corte di giustizia aveva fatto espresso riferimento ai principi sanciti dal diritto internazionale in materia di giurisdizione, in una controversia relativa però alla regolarizzazione dell'attività della pesca[512].

In particolare, durante la fase dei lavori preparatori del regolamento (UE) 2016/679 era stato ipotizzato il rischio che l'Unione europea, esercitando in maniera così estesa la propria giurisdizione, potesse in qualche modo superare i limiti impostegli dal diritto internazionale consuetudinario. In base a quest'ultimo, infatti, è necessario che ci sia "a *bona fide* connection between the subject matter of a dispute and the State asserting jurisdiction over it"[513]. Tradizionalmente, i criteri stabiliti dal diritto pubblico internazionale per l'esercizio della giurisdizione sono: a) principio di territorialità; b) nazionalità (attiva o passiva); c) il principio degli effetti; d) il principio di protezione e, infine, e) il principio di universalità.

Il principio maggiormente utilizzato in tema di giurisdizione è quello della territorialità, applicato anche nel diritto penale[514]. Con esso si attribuisce allo Stato il diritto

[508]Articolo 21, par. 1, TUE "1. L'azione dell'Unione sulla scena internazionale si fonda sui principi che ne hanno informato la creazione, lo sviluppo e l'allargamento e che essa si prefigge di promuovere nel resto del mondo: democrazia, Stato di diritto, universalità e indivisibilità dei diritti dell'uomo e delle libertà fondamentali, rispetto della dignità umana, principi di uguaglianza e di solidarietà e rispetto dei principi della Carta delle Nazioni Unite e del diritto internazionale".
[509]Corte di giustizia, *Air Transport Association of America e altri c. Secretary of State for Energy and Climate Change*, sentenza del 21 dicembre 2011, causa C-366/2010.
[510]*Ibidem*, par. 101.
[511]Cfr. LORAND BARTELS, *The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects*, in *European Journal of International Law* 2015*,* pagg. 1071-1078.
[512]Corte di giustizia, *Cornelis Kramer e altri*, sentenza del 14 luglio 1976, cause riunite 3, 4 e 6/76, parr. 30/33.
[513]B. VAN ALSENOY, *Reconciling the (extra)territorial reach of the GDPR with public international law,* in *Data Protection and Privacy under Pressure – Transatlantic tensions, EU surveillance, and big data,* Maklu 2017, pag. 78.
[514]Vedi, ad esempio, l'articolo 3 del codice penale italiano.

di regolare le persone, gli eventi e tutto ciò che avviene sul suo territorio. L'esercizio della giurisdizione è, infatti, tradizionalmente connesso al concetto di "sovranità", che assume una rilevanza primaria all'interno dell'ordinamento statale, essendo *conditio sine qua* non affinché uno Stato possa essere riconosciuto tale dagli altri appartenenti alla comunità internazionale ed essere, quindi, rispettato nell'esercizio delle funzioni sue proprie. A livello storico, inizialmente si parlava di "sovranità territoriale"[515], identificandosi questa con un diritto reale che lo Stato aveva sul proprio territorio[516]. Questo concetto di sovranità era però adatto ad una realtà storica feudale nel quale lo Stato appariva in veste di Stato "patrimoniale", e, pertanto, è risultato in epoca successiva troppo restrittivo[517]. Con il trascorrere dei secoli, il territorio non costituiva più l'oggetto della sovranità, bensì l'ambito materiale entro il quale i poteri statali venivano esercitati, e solo questi ultimi formavano l'oggetto e il contenuto della sovranità. La sovranità veniva quindi intesa quale diritto ad esercitare in modo esclusivo la propria attività di governo sulla comunità di individui situati nel proprio territorio, e, in quanto attività di tipo coercitivo, implicava anche il potere di escludere qualsiasi interferenza da parte di soggetti terzi .

Anche il fenomeno dell'applicazione extraterritoriale della giurisdizione non è del tutto nuovo nello scenario internazionale. Infatti, mentre sono territoriali tutte le funzioni svolte dallo Stato a titolo esclusivo ed in regime tendenzialmente assoluto nel suo ambito spaziale, in base alla classica tripartizione di funzione legislativa amministrativa e giudiziaria[518], accade che, talvolta, uno Stato eserciti le funzioni pubbliche sul proprio territorio, ma in riferimento a fatti o situazioni verificatesi all'interno del territorio di altro Stato. Questo fenomeno, che va appunto sotto il nome di "applicazione extraterritoriale della giurisdizione", non costituisce un illecito internazionale, essendo l'esclusività del potere dello Stato nel suo territorio riferita solo all'esercizio dell'autorità su persone e beni, cioè alla giurisdizione, ma non anche all'applicazione del diritto.

La Corte permanente di giustizia internazionale si è pronunciata a riguardo nella nota sentenza *Lotus*[519], stabilendo che "la limitazione primordiale che impone il diritto internazionale allo Stato è quella di escludere - salvo l'esistenza di una regola permissiva

[515]Cfr. B. CONFORTI*, Diritto internazionale*, Editoriale Scientifica, Napoli 2018, pag.193
[516]Cfr. R. QUADRI*, Diritto Internazionale Pubblico,* Liguori Editore, Padova 1949, pag. 405.
[517]Cfr. R. LUZZATTO, *Stati stranieri e giurisdizione nazionale*, Giuffré, Milano 1972, pag. 17.
[518]Cfr. M. PANEBIANCO*, Giurisdizione interna e immunità degli Stati stranieri,* Jovene, Napoli 1967, pag.147.
[519]Corte permanente di giustizia internazionale, *Francia c. Turchia, the S.S. Lotus Case,* sentenza del 7 settembre 1927, Serie A, n.10.

contraria - ogni esercizio del potere sul territorio di altro Stato. In questo senso, la giurisdizione è certamente territoriale: essa non potrà essere esercitata fuori dal territorio, se non in virtù di una regola permissiva derivante del diritto internazionale consuetudinario o da una convenzione. Non ne consegue però che il diritto internazionale vieti ad uno Stato di esercitare, nel proprio territorio, la propria giurisdizione in ogni questione in cui si tratta di fatti avvenuti all'estero ed in cui essa possa fondarsi su di una regola permissiva di diritto internazionale".

In generale, si constata sul piano del diritto internazionale contemporaneo la scomparsa di una visione assoluta della territorialità della legge e della giurisdizione, dovuta principalmente all'inserimento di nuove norme volte alla promozione della tutela dei diritti umani, alla cooperazione economica e sociale, alla solidarietà fra i vari popoli. Queste comportano un restringimento della cosiddetta *domestic jurisdiction*, cioè dell'ampia libertà di cui gli Stati godono nell'amministrare il proprio territorio[520]. I limiti alla sovranità dello Stato sono principalmente imposti da norme convenzionali, ma non sono mancati casi in cui le eccezioni derivassero dal diritto consuetudinario. Le prime eccezioni che si sono andate affermando sul piano del diritto pattizio riguardano il trattamento dello straniero e, in particolare, quello degli organi statali e gli agenti diplomatici.

Si può dire, infatti, che il principio di territorialità abbia iniziato ad andare in crisi soprattutto in seguito alla conclusione del secondo conflitto mondiale, quando da un lato si è avvertita come indispensabile l'esigenza di perseguire i gravi crimini internazionali commessi durante i regimi totalitari anche attraverso l'istituzione di tribunali internazionali, e, dall'altro lato, gli individui iniziavano ad essere considerati nel sistema di diritto internazionale come soggetti meritevoli di tutela[521]. Questo processo culminerà nella proclamazione della Dichiarazione universale dei diritti umani nel 1948, il cui ambito di applicazione riguarda, appunto, "tutti i popoli e tutte le Nazioni".

L'articolo 3 del regolamento (UE) 2016/680 costituisce, pertanto, un'eccezione ai tradizionali criteri di territorialità[522], basandosi principalmente sul criterio degli effetti ed

[520]Cfr. B. CONFORTI*, op. cit.*, v. sopra nota 515, pag. 199 ss.
[521]Sul tema cfr., ad esempio, P. L. ZANARDI, G. VENTURINI, *Crimini di guerra e competenze delle giurisdizioni straniere*, Giuffré, Milano 1998.
[522]Cfr. DAN JERKER B. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses,* in *Stanford Journal of International Law* 2014, pag. 61.

estendendo quindi l'ambito di applicazione della normativa comunitaria anche nei confronti degli Stati terzi per quelle situazioni in cui, nella prospettiva del legislatore europeo, gli individui necessitano di una maggiore tutela. Si può ritenere, infatti, che l'estensione extraterritoriale della normativa sia espressione del principio di territorialità (oggettiva), unitamente a quello degli effetti[523]. Proprio quest'ultimo principio, tuttora molto dibattuto nella dottrina, costituirà oggetto di una riflessione critica nel prossimo paragrafo, con riferimento soprattutto alla possibilità di applicarlo nell'ambito delle controversie che possono sorgere in materia di violazioni dei dati personali commesse *online*. Si procederà, pertanto, ad un'analisi sia dei vantaggi che la sua applicazione potrebbe comportare, sia dei rischi connessi ad un possibile abuso da parte degli Stati, i quali potrebbero, in nome dell'estensione universale che caratterizza il ciberspazio, reclamare di essere affetti da un contenuto pubblicato in rete o da un'attività in esso esercitata in qualsiasi parte del mondo.

Occorre, infine, evidenziare che esistono a livello globale altre leggi nazionali in materia di protezione dei dati personali che applicano, a certe condizioni e alla pari del regolamento (UE) 2016/679, il principio di extraterritorialità. Questo è quanto si verifica, ad esempio, negli Stati Uniti, in Brasile e in Australia[524]. Purtuttavia, i suddetti Paesi non costituiranno oggetto di analisi nel presente elaborato, non essendo la protezione dei dati ivi concepita come un diritto fondamentale[525].

[523]B. VAN ALSENOY, *op. cit.*, v. sopra nota 513, pag. 97.
[524]Cfr. C. KUNER, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis*, in *International Journal of Law and Information Technology* 2010, pag. 176. Tra i Paesi citati preme mettere in evidenza la legge americana *Children's Online Privacy Protection Act,* che prevede l'applicazione extraterritoriale della normativa a tutti quei casi in cui i siti *web*, localizzati nel mondo, raccolgano informazioni relative a bambini di nazionalità statunitense.
[525]Cfr. M. TAYLOR, *op. cit*., v. sopra nota 506, pag. 247.

4.2.3 Come riconciliare l'universalità di Internet e il principio territoriale della giurisdizione? Il principio degli effetti come possibile soluzione

Invero, il carattere "universale" di Internet ha fortemente messo in crisi i tradizionali criteri di attribuzione della giurisdizione e di applicazione della legge nazionale, basati principalmente sulla localizzazione della fattispecie[526]. Il venire meno del concetto di territorialità potrebbe produrre conseguenze significative in materia di tutela dei dati personali, dal momento che la maggior parte delle informazioni vengono ormai raccolte, trattate e trasferite proprio sulle piattaforme *online*. Orbene, nonostante l'importanza applicativa della questione, quello dell'esercizio della giurisdizione in materia di dati personali risulta un terreno ancora poco esplorato soprattutto dal punto di vista del diritto internazionale pubblico[527].

Con riguardo, in particolare, alla tutela dei diritti nel ciberspazio, sono state avanzate negli anni due possibili soluzioni: la prima consisteva nella creazione di un sistema giuridico *sui generis,* applicabile a tutte le controversie nascenti dalle attività svolte su Internet e basata sull'idea di un ciberspazio completamente indipendente[528]; la seconda invece, riteneva che fosse più utile uniformare le norme già esistenti in materia di giurisdizione e legge applicabile[529]. Al fine di risolvere, poi, nello specifico i conflitti che potrebbero sorgere in rete, sono stati proposti due possibili approcci, uno di tipo universale – di fatto impraticabile in ragione delle insormontabili differenze tra i vari sistemi legislativi - e uno, invece, più liberale, in cui veniva lasciato a ciascuno Paese un ampio margine su come disciplinare la materia. Anche quest'ultimo approccio presentava, però, diversi punti critici, legati soprattutto all'eventualità che uno Stato, economicamente e tecnologicamente più forte, potesse imporre i propri valori sugli altri[530].

[526]Cfr. U. KOHL, *op. cit.,* v. sopra nota 435, pag. 4.
[527]Cfr. S. BESSON, *op. cit.,* v. sopra nota 475, pag. 588
[528]Cfr. J. PERRY BARLOW, *A Declaration of the Independence of Cyberspace,* 8 febbraio 1996, disponibile alla pagina https://www.eff.org/it/cyberspace-independence.
[529]Cfr. J. ZITTRAIN, *Be Careful What You Ask For: Reconciling a Global Internet and Local Law,* The Berkman Center for Internet & Society Research Publication no. 2003-03, pag. 8.
[530]D. CASTRO, R. ATKINSON, *Beyond Internet Universalism: A framework for Addressing Cross-Border Internet Policy*, The Information Technology & Innovation Foundation, Settembre 2014, disponibile alla pagina http://www2.itif.org/2014-crossborder-internet-policy.pdf, pagg. 8-10.

In ogni caso, l'*Article 29 Working Party* ha recentemente stabilito che le questioni connesse all'esercizio della giurisdizione in materia di protezione dei dati personali debbano essere risolte in base ai criteri stabiliti dal diritto internazionale pubblico[531].
A livello generale, nelle controversie internazionali si possono normalmente distinguere tre tipi di potere in capo agli Stati: il diritto di legiferare, il diritto di giudicare le controversie che presentano elementi di estraneità e, infine, il diritto di far rispettare le leggi e le decisioni[532].

I principi maggiormente diffusi ed accettati nella comunità internazionale per attribuire la giurisdizione ad uno Stato sono, oltre a quello difficilmente praticabile dell'universalità, quello della territorialità - già discusso nel paragrafo precedente e fondato sul caso *Lotus* della Corte permanente di giustizia internazionale – che può essere oggettivamente territoriale o soggettivamente territoriale, quello della personalità, quello di protezione e, infine, quello degli effetti.
Orbene, un'ipotesi applicativa del principio di territorialità è prevista ora dal nuovo articolo 3 regolamento (UE) 2016/679, ma anche gli altri criteri, come quello della personalità, sono stati recentemente applicati in altri contesti. In particolare, quest'ultimo criterio si può fondare sulla personalità attiva (autore dell'illecito) o sul quella passiva (vittima dell'illecito). Un esempio di applicazione del criterio della personalità in questo contesto si poteva infatti riscontrare nella legge nazionale greca che recepiva l'ormai abrogata direttiva 95/46/CE, ove si leggeva nell'articolo relativo all'ambito di applicazione, poi modificato nel 2006 in seguito ad alcune obiezioni avanzate dalla Commissione europea, che l'Autorità Garante greca avesse giurisdizione anche nei confronti di tutti i responsabili del trattamento, che avevano la propria sede al di fuori del territorio nazionale ma trattavano i dati relativi alle persone residenti in Grecia. L'applicazione extraterritoriale della disciplina nazionale si concretizzava nell'obbligo imposto in capo ai responsabili del trattamento di nominare un rappresentante anche in Grecia. Ebbene, dal momento che la maggior parte delle persone residenti in Grecia erano

[531]Article 29 Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, 30 maggio 2002, 5035/01/EN/Final WP 56, pag. 2.
[532]*Ibidem*, pag. 16.

verosimilmente anche cittadini greci, era stato ritenuto che in questo caso l'applicazione extraterritoriale fosse fondata sul criterio della nazionalità degli interessati[533].

Il terzo criterio, invece, il cosiddetto "principio di protezione", si applica soprattutto nell'ambito del diritto penale e si concretizza nella possibilità per lo Stato nazionale di esercitare la giurisdizione e punire le condotte commesse all'estero, ma i cui effetti minacciano la sicurezza e la sovranità nazionale[534]. Un'applicazione di questo principio si può trovare, ad esempio, nell'articolo 7 del codice penale italiano, secondo cui la legge nazionale si applica al cittadino o allo straniero che commettano all'estero gravi reati contro la personalità dello Stato italiano o delitti di contraffazione di monete o sigilli[535].

Viene in rilievo, infine, la "dottrina degli effetti", che giustifica l'esercizio extraterritoriale della giurisdizione sulla base del fatto che le azioni condotte all'estero da parte di autorità statali produrrebbero effetti diretti anche nel territorio nazionale. Le prime applicazioni della suddetta dottrina risalgono agli anni '70, quando le corti statunitensi avevano ritenuto di applicare la legge nazionale in materia di concorrenza anche alle attività commerciali svolte all'estero, ma i cui effetti si producevano sul territorio americano[536].

Uno degli argomenti più dibattuti in dottrina in relazione all'esercizio extraterritoriale della giurisdizione in materia di protezione dei dati personali riguarderebbe, per l'appunto, l'eventuale estensione della giurisdizione anche al cosiddetto "paese di destinazione", in aggiunta al "paese d'origine". La maggiore propensione per l'estensione del criterio degli effetti si giustificherebbe alla luce del fatto che, spesso, il luogo in cui si trova il soggetto – o in questo caso sarebbe più appropriato parlare del luogo in cui si trova l'*Internet service provider* o il soggetto o titolare del trattamento – non corrisponde a quello in cui si producono i danni[537].

Il criterio degli effetti, pur potendo apportare diversi vantaggi in termini di una maggiore tutela dei dati personali, esso, se applicato in contesti come quelli dello scambio

[533]Cfr. C. KUNER, *op. cit.*, v. sopra nota 524, pag. 19.
[534]Cfr. N. LUBELL, *Extraterritorial Use of Force Against Non-State Actors,*Oxford University Press 2010, pag. 208.
[535]Articolo 7 c.p. "Articolo 7. Reati commessi all'estero. È punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati: 1) delitti contro la personalità dello Stato; 2) delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto; 3) delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano; 4) delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni; 5) ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana".
[536]U. KOHL, *op. cit.,* v. sopra nota 435, pagg. 91 e 92.
[537]*Ibidem*, pag. 25.

di dati personali attraverso Internet – che per definizione è transfrontaliero e senza confini territoriali ben definiti – rischierebbe di essere soggetto a possibili abusi da parte degli Stati, i quali potrebbero sempre reclamare di essere "affected by online content or activity originating from anywhere in the world"[538]. A livello legislativo, inoltre, mancherebbero […] any competence rules favouring the country of destination […]"[539].
Si è cercato, pertanto, di proporre una cosiddetta "teoria intermedia degli effetti", che attribuirebbe la giurisdizione solo allo Stato *specificatamente destinatario* delle attività *online.* Tuttavia, anche questo approccio non risulta essere completamente risolutivo[540].

Orbene, nonostante i segnali positivi forniti dal regolamento (UE) 2016/679, si constata come, invece, nel sistema di tutela dei diritti umani previsto dal Consiglio d'Europa, il relativo organo giurisdizionale non si sia ancora pronunciato in merito all'eventuale applicazione extraterritoriale dell'articolo 8 CEDU. In questo contesto, infatti, la giurisdizione si fonda ancora principalmente sul criterio del controllo effettivo, sul territorio o sulle persone: "the state obligation to respect human rights is not limited territorially; however, the obligation to secure or ensure human rights is limited to those areas that are under the state's effective overall control"[541].
La situazione sembra apparire, invece, più favorevole nel sistema di tutela interamericano, in ragione soprattutto del citato parere reso dalla Corte interamericana dei diritti umani nel 2017, ove si è fatto ricorso al criterio degli effetti anche in materia di tutela dei diritti umani e, nello specifico, in caso di danni ambientali. In base a questo principio, uno Stato potrebbe, infatti, "[…] regulate behavior which takes place outside its territory insofar as it produces substantial effects within its territory"[542].

Sempre a livello legislativo, nel 2008 un gruppo di esperti in materia, guidati dall'Autorità Garante per la protezione dei dati spagnola, aveva presentato in occasione della 30sima Conferenza Internazionale dei Commissari dei dati personali e della privacy

[538]*Ibidem*, pag. 93. Cfr. anche J. ZITTRAIN, *op. cit.,* v. sopra nota 529, pagg. 1-15.
[539]Cfr. KOHL, *op. cit*., v. sopra nota 435, pag. 25
[540]*Ibidem*, pag. 26.
[541]M. MILANOVIC, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal* 2015, pag. 263.
[542]B. VAN ALSENOY, *op. cit.,* v. sopra nota 513, pag. 92.

una *Joint Proposal for setting International Standards on Privacy and Personal Data Protection*[543], la quale prevedeva all'articolo 25, "Applicable Law and Jurisdiction", che:

> "1. The processing of personal data will be governed by the applicable law and the competent tribunal of the State in which territory the responsible person has an establishment, within the framework of whose activities the processing is carried out.
> In those cases where the responsible person has no establishment in a State but addresses its activity specifically to its territory, processing of personal data carried out under such activity will be governed by the applicable law and the competent tribunal of that State.
> In the context of this paragraph establishment shall mean any stable facility that allows the real and effective exercise of an activity, regardless of their legal form".

Questa disposizione, che di fatto attribuiva la giurisdizione in base al criterio del luogo del domicilio o della sede del responsabile del trattamento, è stata poi abrogata nella versione definitiva della proposta.
In mancanza di un adeguato sistema normativo internazionale, sono stati pertanto identificati i tre criteri principali su cui eventualmente fondare la giurisdizione statale in caso di controversie relative ad atti compiuti nel ciberspazio. In particolare, 1) è necessario che ci sia una connessione sostanziale tra la questione controversa e lo Stato che rivendica la giurisdizione; 2) lo Stato deve avere un legittimo interesse nella questione e, infine, 3) l'esercizio della giurisdizione è ragionevole, tenuto conto della proporzionalità fra gli interessi statali e gli altri interessi in gioco[544].

In conclusione, malgrado le diverse ipotesi formulabili a livello teorico, permangono numerose lacune nel quadro giuridico internazionale in relazione all'esercizio della giurisdizione e all'indicazione dei criteri per l'applicazione extraterritoriale delle leggi in materia di tutela dei dati personali. Conseguentemente, sorge spontaneo domandarsi se quello territoriale resti pur sempre l'unico criterio nel concreto praticabile, escludendo quindi qualsiasi esercizio extraterritoriale giurisdizione in caso di violazione del diritto alla privacy *online*[545].

---

[543]*Joint Proposal for setting International Standards on Privacy and Personal Data Protection*, disponibile alla pagina https://www.garanteprivacy.it/documents/10160/10704/1707373.
[544]Cfr. DAN JERKER B. SVANTESSON, *A new legal framework for the age of cloud computing*, disponibile alla pagina https://theconversation.com/a-new-legal-framework-for-the-age-of-cloud-computing-37055.
[545]Cfr. U. KOHL, *op. cit.,* v. sopra nota 435, pag. 164.

CAPITOLO 5
VERSO L'ADOZIONE DI NUOVE SOLUZIONI

5.1 LE SOLUZIONI AVANZATE A LIVELLO INTERNAZIONALE ED EUROPEO 5.1.1 La crittografia 5.1.2 L'anonimizzazione 5.1.3 L'anonimizzazione e la crittografia nel sistema di tutela internazionale dei dati personali 5.1.4 L'anonimizzazione e la crittografia nel sistema europeo di tutela dei dati personali 5.2 L'OBBLIGO DI NOTIFICA E IL "DATA BREACH" 5.3 UN POSSIBILE SUPERAMENTO DEL CONFLITTO PRIVACY/SICUREZZA NAZIONALE?

5.1 LE SOLUZIONI AVANZATE A LIVELLO INTERNAZIONALE ED EUROPEO

Nel precedente capitolo sono stati affrontati i problemi relativi all'eventuale imputazione di responsabilità delle società di diritto privato in caso di violazione dei dati personali degli utenti, nonché quelli relativi all'esercizio extraterritoriale della giurisdizione da parte degli organi internazionali di controllo. Questo capitolo sarà dedicato, invece, alla descrizione delle diverse tecniche proposte a livello internazionale ed europeo anche al fine di rafforzare la tutela della privacy.

Invero, la maggior parte delle comunicazioni avvengono oggigiorno quasi esclusivamente attraverso applicazioni collegate a Internet (Whatsapp, Skype, Facebook). Su queste piattaforme gli utenti scambiano milioni di informazioni, molte di natura anche sensibile quali opinioni politiche, religiose o informazioni relative alle attività lavorative svolte. Tutte le informazioni condivise sulle piattaforme *online* costituiscono, allo stesso tempo, dati personali utili da raccogliere e trattare da parte delle autorità di *law enforcement*, le quali possono in questo modo accedere non solo al contenuto delle informazioni, ma anche ai dati anagrafici, alle password, alla localizzazione ecc. Al fine di arginare i possibili abusi da parte dei governi statali, i quali hanno spesso fatto ricorso negli ultimi anni a programmi di sorveglianza di massa, risulta fondamentale per le società che forniscono questi tipi di servizi implementare le diverse tecniche per criptare e anonimizzare i dati raccolti e tutelare in maniera effettiva la privacy degli utenti. Alcuni autori hanno addirittura affermato che in una società come quella americana, in cui il diritto alla privacy è stato negli ultimi anni fortemente indebolito in seguito alla promulgazione del Patrioct Act, "the ubiquitous usage of strong encryption can help restore the balance between privacy and security"[546].

[546]D. J. SHERWINTER, *Surveillance's slippery slope: using encryption to recapture privacy rights,* in *Journal on Telecommunication & High Technology Law* 2007, pag. 502. Ricorrere alla crittografia permette non solo di difendersi dalla sorveglianza ingiustificata dei governi, ma anche da quella effettuata dalle compagnie private per finalità di lucro.

5.1.1 La crittografia

La crittografia è una tecnica molto antica – le prime tracce di questo strumento si rinvengono già prima della nascita di Cristo al tempo dei Babilonesi - e consiste nel "cifrare" un certo messaggio, rendendolo comprensibile solo al suo destinatario. Letteralmente il termine deriva dalle parole greche "criptos", ossia nascosto, e "grafia", che significa parola. Il messaggio da decifrare si chiama invece crittogramma. La crittografia è stata inoltre definita dall'Organizzazione per la cooperazione e lo sviluppo economico come "[…] a discipline that embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use. It is one of the technological means to provide security for data on information and communications systems"[547]. Questa scienza coinvolge la matematica, l'ingegneria, le scienze informatiche e, recentemente, si stanno iniziando a studiare anche gli effetti di essa sulla tutela dei diritti umani.

I tre principali metodi per crittografare sono quello classico, rotante e digitale[548]. Il primo metodo veniva già utilizzato dalla civiltà Babilonese nell'VIII secolo A.C. e si è poi largamente diffuso all'epoca di Giulio Cesare – di cui si ha testimonianza attraverso il famoso cifrario di Cesare, considerato uno dei più antichi algoritmi crittografi rinvenuti nella storia. Esso serviva ad inviare messaggi di guerra e utilizzava algoritmi trasposti o sostitutivi. In altre parole, il contenuto dell'informazione veniva criptato attraverso l'utilizzo di un codice segreto, per cui ogni lettera dell'alfabeto veniva sostituita con un'altra appartenente all'alfabeto segreto. Ad esempio, si poteva decidere che il codice segreto consistesse nel fare slittare le lettere dell'alfabeto di due posizioni l'una, trasformando cosi la parola "casa" in "ecvc".

Successivamente venne introdotta una variante del cifrario di Cesare, il cosiddetto cifrario di Vigenère risalente al XVI secolo D.C., che prevedeva lo spostamento delle lettere da cifrare per un numero variabile di posti, stabilito in base ad un codice, detto anche verme, conosciuto solo all'emittente e al destinatario.

Il mondo della crittografia è rimasto pressoché invariato fino alla prima guerra mondiale, quando, sempre per ragioni belliche, è stato introdotto il metodo della crittografia rotante, che si avvaleva di strumenti meccanici, e non più manuali, per criptare e decriptare i

[547]UNESCO SERIES ON INTERNET FREEDOM, *Human Rights and encryption,* pag. 9, disponibile alla pagina: http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.
[548]Cfr. D. J. SHERWINTER, *op. cit.*, v. sopra nota 546, pag. 512.

messaggi segreti inviati dagli Stati nemici. L'esempio più famoso è costituito senza dubbio dalla macchina *Enigma*, un cifrario polialfabetico.
Infine, negli ultimi anni si è sviluppata la cosiddetta crittografia digitale, che si avvale, di computer e altri strumenti tecnologici per creare complessi algoritmi in grado di cifrare e decifrare messaggi, importanti anche per la sicurezza di ogni nazione.

In generale, i due processi che vengono applicati a qualsiasi tecnica crittografia sono la "cifratura", che lavora sulle singole lettere dell'alfabeto, e la "codifica", che lavora ad un livello semantico più alto come una parola o una frase.

Ogni sistema di crittografia consta di due parti essenziali: 1) un algoritmo per codificare e decodificare e 2) una "chiave", che consiste in una serie di informazioni che, combinate con il testo non criptato, passato attraverso l'algoritmo, darà il testo codificato. Ci sono due elementi che determinano l'efficacia della chiave, ossia la capacità di rimanere segreta e la sua lunghezza.
La crittografia può essere di due tipi:

1) Simmetrica o a chiave privata, quando un'unica chiave viene utilizzata sia per la firma dei documenti sia per la verifica;
2) Asimmetrica o a chiave pubblica, quando viene utilizzata una chiava privata per la firma dei documenti e una pubblica per la loro verifica

Il più diffuso algoritmo di crittografia simmetrica è il DES (*Data Encryption Standard),* inventato nel 1970 e divenuto l'algoritmo standard utilizzato dal governo americano[549].

Recentemente è stata introdotta un'ulteriore tecnica di crittografia, nota con il nome di crittografia omomorfa, e viene utilizzata soprattutto nel *cloud computing.* Essa permette di effettuare dei calcoli sui numeri cifrati senza decifrarli. Il risultato criptato infatti, quando decriptato, è uguale al risultato della computazione eseguita sui messaggi non criptati. Non ricorrere mai alla decifrazione garantisce una maggiore sicurezza dei dati personali.
La crittografia *end-to-end*, la forma più diffusa della "crittografia a chiave pubblica", è stata invece introdotta per la prima volta dall'applicazione Telegram e ora utilizzata anche da Whatsapp e altre società di comunicazione. In particolare, si può registrare un evidente incremento della sua utilizzazione soprattutto in seguito alle rivelazioni di Snowden nel 2013[550]. Questa tecnica si basa su due chiavi, una pubblica, che è la chiave che cripta, e una

[549]Cf. A. CILLI, *Manuale del Web*, *Tecnologie, normative e management,* Franco Angeli, 2004 Milano, pag. 109.
[550]UNESCO SERIES ON INTERNET FREEDOM, *Human Rights and encryption,* disponibile alla pagina: http://unesdoc.unesco.org/images/0024/002465/246527E.pdf.

privata, che invece la chiave necessaria per decriptare. Poniamo ad esempio una comunicazione fra due individui A e B. A invierà la chiave pubblica a B, il quale a sua volta digiterà il messaggio che vuole inviare ad A. Grazie alla chiave pubblica il messaggio, una volta digitato, verrà criptato in modo che neanche B potrà più tornare al testo originario. Il messaggio, così criptato, verrà inviato a A, il quale, grazie alla chiave segreta posseduta solo da lui, potrà decifrarlo. La chiave pubblica solitamente è simile a quella privata ma molto più breve.

5.1.2 L'anonimizzazione

L'anonimizzazione è una tecnica finalizzata a rendere irreversibile l'identificazione di una persona. Essa consta tradizionalmente di due fasi: nella prima vengono eliminati dai gruppi di dati tutte le caratteristiche di identificazione personale (PII), come nome, indirizzo, data di nascita o numero di previdenza sociale; nella seconda fase, invece, vengono modificate o eliminate altre categorie di dati che potrebbero agire come identificatori in quel particolare contesto - che potrebbero essere, ad esempio, per una banca i numeri delle carta di credito, o per un'università, invece, i numeri di matricola degli studenti[551]. Una volta anonimizzati, i dati possono essere ancora analizzati, condivisi o messi a disposizione del pubblico, ma allo stesso tempo gli individui, non potendo essere più identificati, sono tutelati dal punto di vista della privacy. Tuttavia, con l'evolversi degli strumenti informatici, è diventato sempre più complesso riuscire ad anonimizzare in maniera totale e definitiva i dati. Combinando infatti i diversi gruppi di dati tra di loro, è possibile in molti casi risalire ancora all'identificazione del soggetto cui i dati personali si riferiscono.
A questo proposito, la *Federal Trade Commission* degli Stati Uniti aveva infatti dichiarato nel 2012 che:

"There is significant evidence demonstrating that technological advances and the ability to combine disparate pieces of data can lead to identification of a consumer, computer, or device even if the individual pieces of data do not constitute PII"[552].

In ogni caso, l'utilizzo delle tecniche di anonimizzazione si basa sull'assunto che i dati personali siano stati precedentemente raccolti e trattati in conformità alla legislazione

[551]Cfr. E. GIL, *Big data, privacidad y protección de datos*, Agencia Estatal Boletín Oficial del Estado Madrid, 2016, pag.83.
[552]Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, disponibile alla pagina https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf., pag. 20.

applicabile in materia che, per quanto riguarda ad esempio il diritto, è rappresentato ora dal regolamento 2016/679.

5.1.3 L'anonimizzazione e la crittografia nel sistema di tutela internazionale dei dati personali

Il problema del bilanciamento tra le diverse tecniche di crittografia e anonimizzazione e le necessità di sicurezza nazionale e *law enforcement* costituisce tuttora un terreno di discussione molto delicato e controverso in seno alla comunità internazionale e non solo. Infatti, se da un lato queste tecniche permettono agli utenti di comunicare in maniera privata su qualsiasi piattaforma *online*, dall'altro lato, esse impediscono alle autorità di polizia di identificare, ed eventualmente perseguire, gli autori di fattispecie illecite. Questo si rende evidente, ad esempio, nell'ambito del riciclaggio di denaro, ove "widespread availability of strong encryption technology threatens to undermine the effectiveness of the money laundering controls currently in place"[553].

Il problema si pone, in particolare, tutte le volte in cui le attività investigative siano state condotte nel rispetto di tutte le condizioni sostanziali e procedurali previste dall'ordinamento statale, ma ciononostante l'accesso ai dati non sia reso possibile dalla crittografia. In questi casi potrebbero sorgere infatti questioni sulle possibili implicazioni e conseguenze negative in materia di pubblica sicurezza e sulla sicurezza nazionale. La questione non è di facile soluzione e risulta, pertanto, tuttora dibattuta.

Le maggiori perplessità sorgono soprattutto con riferimento alla crittografia, che è passata negli ultimi anni dall'essere utilizzata esclusivamente come tecnica per facilitare le operazioni militari e di *intelligence*, ad essere comunemente diffusa nella tecnologia quotidiana di ogni individuo, garantendo la segretezza delle email, delle comunicazioni vocali e delle immagini, e di tutti i dati salvati e conservati nei *cloud* dei computer.

A livello di tutela internazionale dei diritti umani, nel rapporto dello *Special Rapporteur* sulla Privacy del 2017 veniva auspicato, tra le altre cose, che "[…] Data always in encrypted state – encrypted data can be read only by those who know the decryption key"[554]. Criptare le informazioni *online* permetterebbe, infatti, di tutelare non solo il diritto

[553]A. RUEDA, *The implications of Strong Encryption Technology on Money Laundering,*in *Albany Law Journal Of Science & Technology* 2001*,* pag. 4.
[554]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, *Joseph A. Cannataci*, 34esima sessione, 27 febbraio-24 marzo 2017, A/HRC/34/60, par. 114.

alla privacy, ma altri diritti altrettanto importanti come la libertà di associazione, di espressione o di professare una religione.

In particolare, è proprio con riguardo alla libertà di espressione che negli ultimi anni è stata evidenziata l'importanza della tecnica dell'anonimizzazione. Nel rapporto del 2013 sugli effetti della sorveglianza dei governi sui diritti alla privacy e alla libertà di espressione[555], lo *Special Rapporteur* sulla libertà di espressione Frank La Rue esortava gli Stati ad adottare tutte le misure necessarie per impedire che le società di diritto privato potessero adottare ulteriori misure lesive della privacy e dell'anonimato degli utenti e, allo stesso tempo, in grado di favorire la sorveglianza delle autorità statali, anche attraverso il divieto di ricorrere alla crittografia[556]. Il successivo *Special Rapporteur* David Kaye pubblicava nel 2015 un altro importante contributo sul tema, un rapporto dedicato esclusivamente all'uso della crittografia e dell'anonimato nella comunicazione digitale. Il rapporto riguardava principalmente l'impatto delle due tecniche sulla libertà di espressione, ma è risultato interessante sotto diversi profili anche per la protezione dei dati personali.

Ivi, in particolare, veniva evidenziato che:

"Encryption and anonymity, *today's leading vehicles* for online security, provide individuals with a means to protect their privacy, empowering them to browse, read, develop and share opinions and information without interference and enabling journalists, civil society organizations, members of ethnic or religious group, those persecuted because of their sexual orientation or gender identity, activists, scholars, artists and others to exercise the rights to freedom of opinion and expression"[557].

Invero, il *web* rappresenta oggi spazio ove anche le diverse attività terroristiche e criminose vengono poste in essere, che potrebbe venire oscurato dall'utilizzo della crittografia e dell'anonimizzazione. Tuttavia, sempre secondo lo *Special Rapporteur*, indebolire la crittografia condurrebbe, al contempo, a conseguenze negative anche in termini di tutela dei diritti dei singoli, in quanto un sistema di comunicazione non criptato e indebolito costituisce un terreno favorevole al compimento di attività illecite da parte di attori non statali ed organizzazioni criminose[558].

In base al suddetto rapporto, inoltre, la crittografia proteggerebbe il contenuto delle comunicazioni, ma non oscurerebbe invece altre informazioni, altrettanto utili per le autorità di *law enforcement* e soggetti terzi, quali l'indirizzo IP, sempre a condizione che l'utente

[555]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, 23esima sessione, 17 aprile 2013, A/HRC/23/40.
[556]*Ibidem*, par. 96.
[557]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* 29esima sessione, 22 maggio 2015, A/HRC/29/32, par. 1.
[558]*Ibidem*, parr. 8 e 9.

non abbia fatto anche ricorso alla tecnica dell'anonimizzazione. In questi casi, infatti, potrebbe diventare davvero difficile, se non addirittura impossibile, risalire alla sua identità. Si consideri, però, che le autorità governative hanno pur sempre a disposizione altri strumenti per svolgere le proprie attività investigative al di fuori della sorveglianza elettronica, quali le intercettazioni telefoniche, le informazioni relative alla localizzazione, la sorveglianza fisica (pedinamento) e molte altre ancora.

Per quanto riguarda, in particolare, la tecnica dell'anonimizzazione, "has been recognized for the important role it plays in safeguarding and advancing privacy, free expression, political accountability, public participation and debate"[559], nonostante non si faccia espresso riferimento alla stessa in alcuna delle fonti internazionali che tutelano i diritti umani. Inoltre, sia lo *Special Rapporteur* per la libertà di espressione che la Commissione interamericana dei diritti umani hanno riconosciuto che "the right to freedom of thought and expression and the right to private life protect anonymous speech from government restrictions"[560].

Pertanto, dal momento che l'anonimizzazione favorisce la libertà di opinione e di espressione, gli Stati devono attivarsi per potenziare la suddetta tecnica, o quanto meno impedire che questa venga in qualche modo limitata. Nel rapporto viene anche fatto richiamo alla recente sentenza resa dalla Corte europea dei diritti umani nel caso *Delfi c. Estonia*[561], ove era stata riconosciuta la responsabilità degli *Internet service provider* per la pubblicazione di alcuni commenti diffamatori da parte di utenti anonimi sulle piattaforme *online* gestite dalle società di comunicazione. In questo contesto viene infatti riconosciuto un ruolo importante anche alle società di diritto privato, soprattutto per quanto riguarda le tecniche di anonimizzazione e crittografia anche alla luce del loro sempre più frequente coinvolgimento nelle attività di intermediazione, collaborazione e raccolta dei dati per le autorità di *law enforcement.*

In ogni caso, tutte le limitazioni alla crittografia e alle altre tecniche finalizzate a garantire la segretezza delle comunicazioni sono considerate delle interferenze gravi nei diritti alla privacy e alla libertà di espressione sanciti, rispettivamente, dagli articoli 17 e 19 del Patto sui diritti civili e politici e dagli articoli 8 e 10 CEDU[562]. Conseguentemente,

[559]*Ibidem,* par. 47.
[560]*Ibidem*, par. 47.
[561]Corte europea dei diritti umani (GC), *Delfi c. Estonia*, sentenza del 16 giugno 2015, ricorso n. 64569/09.
[562]UNESCO SERIES ON INTERNET FREEDOM, *Human Rights and encryption,* disponibile alla pagina: http://unesdoc.unesco.org/images/0024/002465/246527E.pdf., pag. 60.

queste limitazioni sono legittime solo se previste dalla legge, sono necessarie alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, e alle altre finalità previste dalle clausole di limitazione, e sono proporzionate alle finalità perseguite[563].

Infine, il rapporto esorta gli Stati ad adottare tutte le misure necessarie per proteggere la privacy delle persone nella comunicazione digitale, attraverso soprattutto il rinforzamento delle tecniche della crittografia e anonimizzazione al fine di contrastare la diffusa sorveglianza tecnologica.

5.1.4 L'anonimizzazione e la crittografia nel sistema europeo di tutela dei dati personali

A livello legislativo europeo, ad oggi, nonostante sia il considerando 26 del regolamento (UE) 2017/679 che l'analogo considerando 26 della precedente direttiva 95/46/CE facciano espresso riferimento all'anonimizzazione[564] - essa viene ivi richiamata quale limite all'applicazione della normativa europea - la suddetta tecnica è ancora priva di regolamentazione normativa[565]. Inoltre, sempre a livello europeo, già la direttiva sulle comunicazioni elettroniche faceva riferimento nell'articolo 6 all'anonimizzazione dei dati[566], e una norma analoga è prevista ora dall'articolo 7 della proposta di regolamento *e-privacy*. In particolare, in base a quanto disposto dall'articolo 7 della proposta di regolamento *e-*

[563]Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye*, 29esima sessione, 22 maggio 2015, A/HRC/29/32, par. 15.
[564]Considerando 26 regolamento (UE) 2016/679:"considerando che i principi della tutela si devono applicare a ogni informazione concernente una persona identificata o identificabile; che, per determinare se una persona è identificabile, è opportuno prendere in considerazione l'insieme dei mezzi che possono essere ragionevolmente utilizzati dal responsabile del trattamento o da altri per identificare detta persona; che i principi della tutela non si applicano a dati resi anonimi in modo tale che la persona interessata non è più identificabile; che i codici di condotta ai sensi dell'articolo 27 possono costituire uno strumento utile di orientamento sui mezzi grazie ai quali dati possano essere resi anonimi e registrati in modo da rendere impossibile l'identificazione della persona interessata". Anche la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche faceva riferimento al considerando 9 all'"anonimizzazione" e ai "dati anonimi": "È opportuno che gli Stati membri, i fornitori e gli utenti interessati, come pure gli organi comunitari competenti, cooperino all'introduzione e allo sviluppo delle tecnologie pertinenti laddove ciò sia necessario per realizzare le garanzie previste dalla presente direttiva, tenuto debito conto dell'obiettivo di ridurre al minimo il trattamento dei dati personali e di utilizzare dati anonimi o pseudo- nimi nella misura del possibile".
[565]I rischi comuni a qualsiasi forma di anonimizzazione sono: 1) l'individuazione, ossia la possibilità di isolare alcuni o tutti i dati che identificano una persona all'interno dell'insieme di dati; 2) correlabilità, ossia la possibilità di correlare almeno due dati concernenti la medesima persona interessata o un gruppo di persone interessate (nella medesima banca dati o in due diverse banche dati); 3) deduzione, vale a dire la possibilità di desumere, con un alto grado di probabilità, il valore di un attributo dai valori di un insieme di altri attributi.
[566]Articolo 6, par. 1, direttiva 2002/58/CE "I dati sul traffico relativi agli abbonati ed agli utenti, trattati e memorizzati dal fornitore di una rete pubblica o di un servizio pubblico di comunicazione elettronica devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, fatti salvi i paragrafi 2, 3 e 5 del presente articolo e l'articolo 15, paragrafo 1".

privacy, sussiste un obbligo per il fornitore di servizi di comunicazioni elettroniche di cancellare o anonimizzare i metadati quando essi non sono più necessari per le comunicazioni, salvo i casi in cui siano necessari per mantenere o ripristinare la sicurezza delle reti e dei servizi di comunicazione elettronica o rilevare problemi o errori tecnici nella trasmissione di comunicazioni elettroniche, oppure se l'utente finale ha prestato il suo consenso al trattamento dei metadati delle sue comunicazioni per uno o più fini specificati, compresa l'erogazione di servizi di traffico a tali utenti finali, purché il o i fini in questione non possano essere realizzati mediante un trattamento anonimizzato delle informazioni.

Al fine di fornire alcune chiarificazioni in una materia ancora priva di un'espressa disciplina normativa, l'*Article 29 Working Party (WP29*), l'organo consultivo istituito ai sensi della direttiva 95/46/CE, ha reso un parere il 10 aprile 2014 circa l'importanza rivestita dall'anonimizzazione nel contesto europeo[567]. Nonostante il suddetto parere non abbia efficacia vincolante, esso è rappresentativo della posizione assunta a riguardo dalle diverse autorità garanti privacy, e dai relativi organi consultivi, in seno degli Stati membri.

Secondo quanto indicato nel documento, esistono due diversi tipi di anonimizzazione, il primo si basa sulla randomizzazione, mentre il secondo sulla generalizzazione.

In particolare, alla famiglia della randomizzazione appartengono tutte le tecniche utilizzate per modificare la veridicità dei dati, al fine di eliminare la correlazione che esiste tra questi e la persona. Le principali tecniche di randomizzazione sono: a) Aggiunta del rumore statistico: consiste nel modificare gli attributi contenuti nell'insieme di dati in modo tale da renderli meno accurati; b) Permutazione: consiste nel mescolare i valori degli attributi all'interno di una tabella in modo tale che alcuni di essi risultino artificialmente collegati a diverse persone interessate; c) Privacy differenziale (o tecnica c.d. *noise injection*): consiste nell'inserire nelle informazioni di una certa quantità "rumore" allo scopo di nascondere l'identità di chi ha generato i dati.

La generalizzazione rappresenta, invece, il secondo gruppo delle tecniche di anonimizzazione, le quali hanno appunto lo scopo di generalizzare gli attributi delle persone interessate, modificando la rispettiva scala o ordine di grandezza - vale a dire, ad esempio, una regione anziché una città, un mese anziché una settimana. Le principali tecniche di generalizzazione sono: a) aggregazione e K-anonimato: le suddette tecniche sono volte a impedire l'individuazione di persone interessate mediante il loro raggruppamento con almeno k altre persone. A tale scopo, i valori degli attributi sono sottoposti a una

[567]Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2015, 0829/14/EN WP216.

generalizzazione tale da attribuire a ciascuna persona il medesimo valore; b) L-L-diversità/T-vicinanza: la l-l-diversità amplia il k-anonimato facendo sì che in ciascuna classe di equivalenza ogni attributo abbia almeno l valori diversi. La t-vicinanza rappresenta un affinamento della l-l-diversità nel senso che mira a creare classi equivalenti che assomigliano alla distribuzione iniziale di attributi nella tabella.

Viene menzionata, infine, la tecnica della pseudonimizzazione, che consiste nel sostituire un attributo (solitamente un attributo univoco) di un dato con un altro dato causale, che non può essere decifrato, così che non si possa risalire al soggetto al quale il dato originario si riferisce. Orbene, sebbene i dati pseudonimizzati siano tradizionalmente considerati anonimi, in realtà questa tecnica non può essere ricondotta alle diverse tecniche di anonimizzazione, dal momento che la persona resta, seppur indirettamente, identificabile[568]. Pertanto, attualmente si ritiene che i dati pseudonimizzati siano ancora dati personali e soggetti, quindi, alle relative norme in materia. In particolare, per quanto riguarda la disciplina europea, in base all'articolo 4, par.1 punto 5 regolamento (UE) 2016/679, sono considerati pseudonimizzati tutti quei dati personali che "[…] non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile".

Le tecniche più diffuse di pseudonimizzazione sono la crittografia a chiave segreta, la funzione crittografica di *hash* e la tokenizzazione.

[568]Cfr. E. GIL, *op. cit.*, v. sopra nota 551, pag. 83.

5.2 L'OBBLIGO DI NOTIFICA E IL "DATA BREACH"

In seguito al recente rinforzarsi delle misure di sorveglianza di massa da parte dei governi, un argomento molto dibattuto nella dottrina e giurisprudenza internazionale ed europea ha riguardato la possibilità di introdurre il meccanismo della notifica a favore dei soggetti destinatari delle misure di interferenza.

A livello europeo, già nel 1987 il Consiglio d'Europa aveva previsto all'articolo 2.2 della raccomandazione R (87) l'obbligo di notifica successiva nei confronti degli individui destinatari di misure di sorveglianza. Nell'ambito nazionale, invece, prima dell'entrata in vigore del regolamento (UE) 2016/679 "While some Member States follow a quite transparent approach, others are more reluctant. The developments in the Member States, however, show a general tendency towards the establishment of a right to be informed"[569]. Inoltre, anche livello giurisprudenziale, la Corte europea dei diritti umani, a partire dalle sentenze analizzate nel terzo capitolo *Klass e altri c. Germania*[570] e *Weber e Saravia c. Germania*[571], ha sempre evidenziato l'importanza della notifica, anche quale strumento strettamente connesso al diritto ad un rimedio giurisdizionale effettivo. Al fine di adattarsi alle sopracitate sentenze della Corte di Strasburgo, ove era stato riconosciuto il sistema di intercettazioni nazionale non conforme agli standard di tutela previsti dall'articolo 8 CEDU, il legislatore tedesco ha in seguito introdotto un sistema di notifica che ha rappresentato per molti anni "[…] the most far reaching notification duty introduced in Europe [….]"[572]. In particolare, in base a quanto dall'articolo 101, par. 4, l'obbligo di notifica sussiste non solo nei confronti dei soggetti diretti destinatari delle misure di intercettazione, ma anche di tutti coloro che sono solo potenziali destinatari.

Nel regolamento (UE) 2016/679 l'obbligo di notifica al soggetto interessato è previsto sia in caso di rettifica o cancellazione dei dati personali o limitazione del trattamento ai sensi degli articoli 16, 17 e 18, sia in caso di violazione dei dati personali, il cosiddetto "data breach", di cui agli articoli 33 e 34. In quest'ultimo caso, infatti, la notifica deve essere effettuata all'autorità di controllo o, nel caso in cui sussistano rischi elevati per i diritti e le libertà delle persone fisiche, direttamente al soggetto interessato. Un'analoga disposizione è prevista anche dall'articolo 30 della direttiva "polizia" (UE) 2016/680 all'articolo 30.

---

[569]P. DE HERT e F. BOEHM, *The Rights of Notification after Surveillance is over: Ready for Recognition?*, *Digital Enlightenment Yearbook 2012,* IOS Press, 2012, pag. 20.
[570]Corte europea dei diritti umani (Plenaria), *Klass e altri c. Germania,* cit.
[571]Corte europea dei diritti umani, *Weber e Saravia c. Germania, cit.*
[572]*Ibidem*, pag. 26.

L'introduzione dell'obbligo di notifica anche in caso di "data breach" rappresenta un'importante novità rispetto a quanto previsto invece dalla precedente direttiva 95/46/CE, che si limitava a prevedere la notifica in caso di trattamento dei dati personali o rettifica o cancellazione[573], ma non in caso di violazione dei suddetti dati. Occorre evidenziare, inoltre, che sia la precedente direttiva che il nuovo regolamento non si applicano nel caso di dati trattati per ragioni di sicurezza nazionale[574].

A livello internazionale, invece, la necessità di prevedere un efficace sistema di notifica è stata anche più recentemente ribadita nei rapporti adottati dallo *Special Rapporteur* sul diritto alla privacy J. Cannatacci – già oggetto di analisi nel primo capitolo del presente elaborato. In particolare, nel penultimo rapporto pubblicato nel febbraio 2017, lo *Special Rapporteur* sottolineava che "[…] that better thought-out and better resourced oversight of intelligence activities is one of the many complementary initiatives that may help improve the protection of the right to privacy world-wide. […]"[575].

5.3 UN POSSIBILE SUPERAMENTO DEL CONFLITTO PRIVACY/SICUREZZA NAZIONALE?

Quest'ultima problematica riguarda la possibilità di superare l'annoso problema del rapporto fra la tutela della privacy e la sicurezza statale, inteso sempre in termini di conflitto "privacy *versus* sicurezza nazionale" valutando, invece, anche il binomio "privacy *con* sicurezza nazionale".

Invero, come già evidenziato con riferimento alle tecniche di crittografia ed anonimizzazione, se da un lato l'abbassamento dei livelli di tutela dei dati personali in rete comporta un più ampio margine di manovra da parte delle autorità di *law enforcement* e dei servizi di sicurezza, dall'altro lato lo stesso ampio margine potrebbe essere, al contempo, sfruttato soprattutto dai *cyberterroristi* e ai *cybercriminali* per compiere atti dannosi nei confronti della società. Proteggere i dati personali ed evitare la loro raccolta indiscriminata potrebbe costituire allora il modo più efficace per tutelare anche la sicurezza nazionale, poiché permetterebbe di limitare il margine di manovra di attività criminose che operano sempre di più attraverso la rete.

[573]Articolo 12, c. 1, lettera b) e articolo 18 direttiva 95/46/CE.
[574]Articolo 3, paragrafo 2, direttiva 95/46/CE; considerando 16 regolamento (UE) 2016/680.
[575]*Ibidem*, par. 3.

Al riguardo occorre sottolineare che, nonostante la dottrina maggioritaria continui a concepire il bisogno di tutelare i dati personali in conflitto con le necessità di tutelare la sicurezza nazionale e l'ordine pubblico – concezione rinforzata dal fatto che, solitamente, anche dal punto di vista storico gli scandali legati alla violazione dei dati personali continuano sortire effetti minori nell'opinione pubblica rispetto a quelli legati agli attacchi terroristici e alle minacce alla pubblica sicurezza - lo *Special Rapporteur* sulla Privacy Joseph Cannatacci abbia, invece, proposto un superamento del contrasto affermando nel rapporto pubblicato nel 2016 che "[…] it is not helpful to talk of "privacy vs. security" but rather of "privacy **and** security" since both privacy and security are desiderata [...] and both can be taken to be enabling rights rather than ends in themselves [...]"[576]. Quest'ultima tesi potrebbe trovare un fondamento non solo a livello pratico, soprattutto in relazione ai casi richiamati di cyberterrorismo, ma anche a livello teorico e dottrinale. E' interessante menzionare in proposito un recente contributo fornito dalla dottrina francese, secondo cui concepire il problema in termini di contrapposizione fra il diritto alla privacy e la sicurezza nazionale/*law enforcement*, si fonderebbe in realtà su un paradosso: uno degli scopi del terrorismo è quello di distruggere lo stato di diritto e minacciare la sicurezza nazionale, anche innescando negli Stati reazioni eccessive e sproporzionate, per cui essi sono portati ad adottare contromisure spropositate e repressive dei diritti degli individui[577]. Gli Stati, pertanto, restringendo i diritti umani, di fatto aiuterebbero a concretizzare gli obiettivi posti in essere proprio dai suddetti terroristici.

In favore della tesi supportata da Sottiaux, viene qui in rilievo anche un'altra dottrina, secondo cui concepire la questione in termini di contrasto tra la tutela dei dati personali e la necessità di garantire la sicurezza nazionale si fonderebbe su presupposti erronei anche dal punto di vista giuridico. Si sarebbe, infatti, giunti negli ultimi anni ad un vero e proprio trade-off "privacy-sicurezza", in ragione di una doppia estremizzazione, da un lato verso l'alto con riguardo alla necessità di tutelare la sicurezza nazionale e, dall'altro lato, verso il basso nei confronti della tutela privacy "becoming an obstacle against achieving the most cherished objective"[578]. Al fine di risolvere il suddetto conflitto, occorre quindi rivalorizzare

[576]Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy,* 31esima sessione, 24 novembre 2016, A/HRC/31/64, par. 24.
[577]Cfr. S. SOTTIAUX, *Terrorism And The Limitations of Rights, the ECHRd the US Constitution,* Hart Publishing 2008, pag. 5.; L. LORELLO, *op. cit.*, v. sopra nota 11, pag. 20.
[578]M. G. PORCEDDA, *The Recrudescence of 'Security v. Privacy' after the 2015 Terrorist Attacks, and the Value of 'Privacy Rights' in the European Union*, in E. ORRÙ, M. G. PORCEDDA e S. WEYDNER-VOLKMANN, *Rethinking Surveillance and Control. Beyond the 'Securityversus Privacy' Debate*, Nomos, Baden Baden2017 (in corso di pubblicazione), pag. 141.

l'importanza che il diritto in questione assume nel sistema legislativo europeo ed internazionale, ove esso include anche il diritto alla vita privata e familiare, la segretezza della corrispondenza, e, soprattutto, costituisce il mezzo attraverso il quale l'identità di un individuo si sviluppa. La suddetta tesi trova la sua base normativa nel fatto che il diritto alla privacy, nella sua più ampia concezione ex articolo 8 CEDU e ex articolo 17 del Patto sui diritti civili e politici, è "strumentale" e fondamentale anche per la tutela di altri diritti, essendo essenzialmente il diritto dell'individuo a manifestare e a sviluppare la sua personalità[579]. Tutelare il diritto in questione permetterebbe infatti il rispetto dello Stato di diritto.

Ad ogni modo, a prescindere dalla posizione che si vuole assumere nel dibattito "privacy/sicurezza nazionale", si riscontra nei diversi sistemi legislativi e giurisprudenziali, analizzati sia a livello internazionale che europeo nel corso del presente elaborato, una positiva tendenza a riconoscere un valore fondamentale al diritto alla protezione dei dati personali e a giudicare tutte le eventuali limitazioni sempre alla luce dei principi di proporzionalità, necessità e legittimità. In proposito, l'avvocato Generale Saugmandsgaard Øe ha infatti affermato nella sua opinione relativa al caso Tele2 Sverige AB che "[…] the requirement of proportionality strictu senso implies weighing the advantages resulting from (a) measure in terms of the legitimate objective pursued against the disadvantages it causes in terms of the fundamental rights enshrined in a democratic society. This particular requirement therefore opens a debate about the values that must prevail in a democratic society and, ultimately, about what kind of society we wish to live in"[580].

[579]Cfr. F. SCHOEMAN, *Privacy: Philosophical Dimensions*, in *American Philosophical Quarterly* 1984, pag. 201.
[580]Corte di giustizia (Grande Sezione) *Tele2 Sverige AB c. Post- och telestyrelsen e Secretary of State for the Home Department c. Tom Watson e altri*, Opinione dell'Avvocato Generale del 16 luglio 2016, cause riunite C-203/15 e C-698/15, par. 248.

CONCLUSIONI

Risulta difficile trarre delle conclusioni in una materia dai contorni ancora indefiniti e in continua evoluzione come quella della protezione dei dati personali. Basti solo pensare che nel lasso di tempo richiesto per la stesura dell'elaborato, a livello europeo, la Corte di giustizia: i) ha dichiarato nella sentenza *Maximilian Schrems* invalido l'accordo commerciale "Safe Harbour" tra l'Unione europea e gli Stati Uniti; ii) sono stati approvati ed entrati in vigore il regolamento (UE) 2016/679 (GDPR) e la direttiva (UE) 2016/680; iii) è stata presentata la proposta di regolamento per le comunicazioni elettroniche. Infine, la Corte europea dei diritti umani si è pronunciata in materia di sorveglianza delle comunicazioni nei casi *Roman Zakharov c. Russia* e *Szabo e Vissy c. Ungheria* e, più recentemente, anche nel caso *Big Brother Watch e altri c. Regno Unito.* A livello internazionale, inoltre, nel 2015 il Consiglio per i diritti umani ha conferito mandato per una durata di tre anni allo *Special Rapporteur* per la privacy, il professor Joseph Cannataci, con la finalità di analizzare la situazione del diritto alla privacy nel mondo ed identificare i principali punti di criticità. Dall'attività di ricerca sono scaturiti tre rapporti, pubblicati ognuno a distanza di circa un anno dall'altro.

Il progetto di ricerca si è posto l'obiettivo di analizzare il diritto alla protezione dei dati personali alla luce delle recenti restrizioni e deroghe poste in essere soprattutto nel contesto europeo ed internazionale in risposta agli attacchi terroristici verificatesi a partire dall'11 settembre 2001. Sono state quindi incluse nell'analisi del diritto alla privacy anche le cosiddette clausole di limitazione, previste a livello internazionale, seppur in maniera implicita, all'articolo 17 del Patto sui diritti civili e politici, e a livello europeo agli articoli 23 regolamento (UE) 2016/679, articoli 13, par. 3, e 15 direttiva (UE) 2016/680, e, infine, all'articolo 52 della Carta dei diritti fondamentali dell'Unione europea.

Nel contesto in esame, il momento di maggiore tensione politica si è registrato nel 2013, quando l'*ex* dipendente dei servizi di intelligenze statunitense (NSA) ha denunciato i programmi di sorveglianza di massa posti in essere dal governo americano, resi possibili anche grazie alla collaborazione di diversi *Internet service provider* americani, nei confronti dei cittadini americani e non solo. In questo momento la comunità internazionale ha infatti acquisito maggiore consapevolezza dei potenziali rischi connessi all'attività di raccolta indiscriminata di informazioni personali da parte delle autorità di sicurezza nazionale e *law enforcement.* Inoltre, la stessa Corte di giustizia ha evidenziato nel caso *Maximilian*

Schrems, seppur in maniera indiretta limitandosi a dichiarare l'accordo internazionale non conforme agli standard riconosciuti dal diritto dell'Unione europea, che il livello di tutela dei dati personali previsto nel sistema legislativo statunitense non fosse sufficientemente adeguato. Invero, sono ancora numerosi gli Stati che concepiscono la sorveglianza di massa come uno degli strumenti più efficaci per tutelare la sicurezza nazionale e prevenire eventuali attacchi terroristici. Queste misure comportano però, allo stesso tempo, notevoli rischi per i diritti degli individui, sia in ragione della mancanza di adeguati controlli giurisdizionali a livello nazionale, sia per la natura spesso indiscriminata dei dati raccolti.
Orbene, nonostante l'importanza assunta dal diritto alla privacy, nel corso del primo capitolo è stata constatata la mancanza di un adeguato sistema legislativo a livello internazionale: invero, l'articolo 12 della Dichiarazione universale dei diritti umani e l'articolo 17 del Patto sui diritti civili e politici non prevedono espressamente la tutela dei dati personali nelle loro disposizioni, né alcuna indicazione è contenuta al riguardo all'art. 8 CEDU. Le lacune normative, dovute principalmente alle ragioni storiche e alla mancanza di adeguate conoscenze tecniche in materia al momento della redazione delle suddette convenzioni e dichiarazioni, sono state in parte compensate dall'evoluzione giurisprudenziale, avutasi soprattutto in seno alla Corte europea dei diritti umani. La mancanza di un'univoca definizione, unitamente al fatto che, solitamente, nel giudizio di bilanciamento tra il diritto alla privacy e la sicurezza nazionale assume un peso maggiore la seconda, il diritto in questione può essere oggetto di numerose violazioni e abusi da parte delle autorità nazionali. Sempre a livello internazionale, inoltre, il rapporto dello *Special Rapporteur* delle Nazioni Unite Frank La Rue sulla promozione e protezione della libertà di opinione ed espressione del 17 aprile 2013 e, più recentemente, i tre rapporti dello *Special Rapporteur* sulla privacy del 2016, 2017 e 2018, hanno evidenziato le implicazioni e i pericoli connessi alla sorveglianza delle comunicazioni sulla libertà di espressione e sul diritto alla privacy.

Sempre a livello normativo, il quadro sembra essere sensibilmente più favorevole nel contesto europeo – oggetto di analisi del secondo capitolo - ove il diritto alla privacy ha acquisito valore di diritto fondamentale grazie all'articolo 8 della Carta dei diritti fondamentali e all'articolo 16 TFUE. Inoltre, il sistema legislativo europeo è l'unico a prevedere una distinzione normativa fra il diritto alla protezione dei dati personali e il diritto alla privacy, tutelati rispettivamente agli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione europea. In generale, si può ritenere che l'Unione europea abbia recentemente dimostrato un significativo interesse al problema della tutela dei dati personali, sia attraverso

le due sentenze analizzate nei casi *Maximilian Schrems* e *Digital Rights Ireland Ltd*, che attraverso l'entrata in vigore del regolamento (UE) 2016/679 e della direttiva "Polizia" (UE) 2016/680 e la proposta di regolamento *e-privacy.* In particolare, tra le più importanti novità introdotte dal regolamento (UE) 2016/679 vengono in rilievo la sua applicazione extraterritoriale ex articolo 3, i concetti di *privacy by design* e *privacy by default*, il diritto alla portabilità dei dati e il cosiddetto "data breach", previsto sia agli articoli 33 e 34 del regolamento che all'articolo 30 della direttiva. Quest'ultimo, in particolare, prevede l'obbligo per il titolare del trattamento di notificare la violazione dei dati all'autorità competente o, nel caso in cui sussista un rischio per i diritti e le libertà delle persone, al soggetto interessato.
In ogni caso, il maggiore contributo interpretativo in materia di tutela dei dati personali e misure restrittive per ragioni di sicurezza nazionale ed esigenze di *law enforcement* è stato fornito dalla Corte europea dei diritti umani in merito alla violazione dell'articolo 8 CEDU. Invero, a partire dal caso *Klass e altri c. Germania* risalente al 1978, relativo a misure di intercettazione da parte delle autorità tedesche, la Corte europea dei diritti umani ha progressivamente stabilito i criteri e le condizioni necessarie per limitare in maniera legittima l'articolo 8 CEDU. In particolare, secondo i giudici di Strasburgo, le limitazioni devono essere previste dalla legge – requisito che nel contesto delle misure di sorveglianza di massa assume una primaria importanza al fine di delimitare il potere discrezionale degli Stati - perseguire uno scopo legittimo, essere necessarie in una società democratica ed essere rispettose del principio di proporzionalità.

La mancanza di un adeguato riferimento normativo, ha reso necessario nel presente elaborato un approccio alla problematica di tipo principalmente giurisprudenziale, constatando anche in questo contesto una tendenza all'instaurazione del cosiddetto "dialogo tra corti". Invero, sono numerosi i richiami effettuati dalla Corte di giustizia alle pronunce di Strasburgo, soprattutto nel caso *Digital Rights Ireland Ltd* con riferimento ai casi *Rotaru c. Romania*, *Liberty e altri c. Regno Unito*, *S. e Marper c. Regno Unito*, e lo stesso è avvenuto nelle sentenze di Strasburgo *Roman Zakharov c. Russia e Zsabo e Vissy c. Ungheria* con riguardo al caso *Digital Rights Ireland Ltd*. Sempre dal punto di vista metodologico, l'analisi delle sentenze è stata condotta principalmente per aree di criticità, mettendo in evidenza gli elementi comuni ai due sistemi giuridici, legati soprattutto all'applicazione della dottrina del margine di apprezzamento e al principio di proporzionalità. Invero, è proprio sulla base del principio di proporzionalità che la Corte di giustizia ha dichiarato

invalida nel 2014 la direttiva 2006/24/CE relativa ai servizi di comunicazione elettronica e, poi, nel 2015 l'accordo commerciale stipulato fra l'Unione europea e gli Stati Uniti, noto con il nome di "Safe Harbour". Con riguardo, invece, alle sentenze della Corte di Strasburgo, una particolare attenzione è stata dedicata alla pronuncia della Grande Camera *Roman Zakharov c. Russia* del 2016, ove è stata constatata, *inter alia*, una maggiore apertura nei confronti del ricorso in astratto, in deroga a quanto previsto dall'articolo 34 CEDU. La maggiore propensione a riconoscere la ricevibilità dei ricorsi in astratto si giustifica in ragione della crescente consapevolezza da parte dei giudici della Corte delle difficoltà riscontrate dai ricorrenti nel dimostrare di essere diretti destinatari delle misure di sorveglianza, data la natura spesso segreta delle stesse. In particolare, sulla base della suddetta deroga è possibile riconoscere lo *status* di vittima sulla base della mera esistenza di misure legislative nazionali. Invero, in base ad una costante giurisprudenza della Corte europea dei diritti umani iniziata a partire dal caso *Klass e altri c. Germania,* e poi ulteriormente ampliata nei successivi casi *Malone c. Regno Unito* e *Association for European Integration and Human Rights e Ekimdzhiev c. Bulgaria*, in materia di sorveglianza delle comunicazioni risulta sufficiente dimostrare, al fine di potere proporre legittimamente ricorso alla Corte per violazione dell'articolo 8 CEDU, la sussistenza del "reasonable likehood", ossia del rischio concreto che il ricorrente possa essere danneggiato dalle misure di sorveglianza. Nel successivo caso *Kennedy c. Regno Unito*, il requisito è stato ulteriormente elaborato, ricomprendendo quale parametro di valutazione anche la disponibilità di eventuali rimedi giurisdizionali a livello nazionale e il rischio concreto che le misure di sorveglianza possano essere applicate nei confronti del ricorrente. Un ulteriore elemento da tenere in considerazione riguarda infatti la categoria di soggetti destinatari delle misure di sorveglianza, risultando maggiormente a rischio coloro che svolgono, ad esempio, delle attività connesse alla tutela dei diritti umani.

Sulla base dell'analisi giurisprudenziale condotta, si è cercato quindi di identificare i tratti comuni al sistema giuridico dell'Unione europea e a quello previsto dalla CEDU in materia di tutela dei dati personali. Invero, la definizione di standard comuni diventa ancora più rilevante se si considera che, ad esempio, in base a quanto stabilito dalla sentenza della Corte di giustizia nel caso *Maximilian Schrems*, i dati personali possono essere trasferiti solo a quei paesi terzi che garantiscono un livello di protezione "essenzialmente equivalente" a quello riconosciuto dall'Unione europea. Sono stati pertanto identificati quali principi comuni ai due sistemi: le specifiche regole sui dati personali e sensibili e sul trasferimento

dei dati verso Paesi terzi, la previsione di un'autorità di controllo indipendente ed imparziale, il controllo giurisdizionale successivo e l'obbligo di notifica, il principio di proporzionalità e, infine, le regole sulle decisioni automatiche e la sicurezza dei dati. Tutti questi standard devono essere rispettati in maniera cumulativa. Interessante inoltre notare un'applicazione, seppur limitata, della dottrina del margine di apprezzamento in questo contesto anche da parte della Corte di giustizia.
In realtà, il fenomeno dei reciproci richiami tra i due organi giurisdizionali non è nuovo nel panorama europeo - potendosi rinvenire i primi casi già nel 1996 nella sentenza *P. c. S. e Cornwall County Council* - ma è interessante evidenziare come quest'ultimo si sia intensificato solo recentemente e non sia più soltanto limitato ai richiami operati dalla Corte di Lussemburgo nei confronti delle sentenze di Strasburgo, giustificati anche a livello normativo dall'articolo 52, par. 3, della Carta dei diritti fondamentali dell'Unione europea, ma anche viceversa, così com'è stato evidenziato nella sentenza *Roman Zakharov* con riferimento alla sentenza *Digital Rights Ireland Ltd.* In quest'ultimo caso, però, i giudici di Strasburgo operano il richiamo pur in mancanza di uno specifico obbligo giuridico al riguardo.

Nel quarto capitolo è stata invece posta l'attenzione su due ulteriori aspetti tuttora irrisolti in materia di protezione dei dati personali, ossia l'eventuale imputazione di responsabilità nei confronti delle società di diritto privato che trasmettono illegittimamente dati personali ai servizi di sicurezza nazionale e alle autorità di *law enforcement,* in violazione degli standard di tutela previsti a livello internazionale per i diritti umani, e l'eventuale esercizio extraterritoriale della giurisdizione da parte degli organi internazionali di controllo. Con riferimento al primo nodo problematico, sono stati analizzati i cosiddetti "transparency reports" pubblicati dai principali *Internet service provider* coinvolti nel programma di sorveglianza statunitense PRISM e, attraverso la creazione di un grafico, è stata constatata la tendenza delle suddette società a trasmettere una quantità sempre maggiore di dati personali alle autorità pubbliche. Il crescente contributo fornito dagli *Internet service provider* alle citate attività rende ancora più pressante il bisogno di creare un sistema normativo uniforme ed adeguato che tuteli i diritti dei singoli. Ciononostante, la disciplina normativa è al momento molto lacunosa, riscontrandosi ad esempio a livello internazionale soltanto un documento, adottato dal Consiglio per i diritti umani nel 2011 intitolato *Guiding Principles on Business and Human Rights*, il quale non fa però espressa menzione al diritto alla privacy, ma si limita in generale ad imporre alle società di condurre

una "human rights due diligence", ossia una valutazione di tutti i potenziali rischi che una determinata operazione può comportare per i diritti umani. Un segnale positivo verso una maggiore consapevolezza dell'eventuale responsabilità delle società di diritto privato in questo contesto è stato senz'altro fornito, a livello europeo, dal regolamento (UE) 2016/679 e dalla proposta di regolamento *e-privacy,* che prevedono rispettivamente al considerando 80 e all'articolo 3, par. 2, l'obbligo per le società che forniscono servizi di comunicazione elettronica che non hanno sede nell'Unione europea, di nominare un rappresentante all'interno del suddetto territorio. Inoltre, anche la Corte di giustizia ha constatato il crescente ruolo svolto dagli *Internet service providers*, pronunciandosi a riguardo nei casi *Digital Rights Ireland Ltd*. e *Tele2Sverige Ab*. Non si rinvengono invece pronunce sul tema da parte della Corte europea dei diritti umani, la quale ha però risolto recentemente altri casi connessi sempre alla violazione del diritto alla privacy ai sensi dell'8 CEDU da parte di soggetti di diritto privato in termini di mancata ottemperanza degli obblighi positivi gravanti sugli Stati in base alla Convenzione.

Per quanto riguarda, invece, la parte dedicata all'eventuale applicazione extraterritoriale dei trattati, constatata la mancanza di pronunce in materia di tutela dei dati personali da parte degli organi internazionali di controllo, è stata condotta un'analisi dell'articolo 3 regolamento (UE) 2016/679, che prevede l'applicazione extraterritoriale della normativa europea anche sulla base del criterio degli effetti, in aggiunta al tradizionale criterio territoriale. L'applicazione del criterio degli effetti potrebbe risultare molto utile in questo contesto, anche alla luce del fatto che spesso il "paese d'origine" e il "paese di destinazione" dell'atto lesivo del diritto alla privacy non coincidono. Allo stesso tempo, però, il suddetto criterio potrebbe essere soggetto ad eventuali abusi da parte degli Stati, che potrebbero reclamare di essere affetti da contenuti *online* da chiunque in qualunque parte del mondo.

In ogni caso, dall'analisi condotta in merito alla principale giurisprudenza della Corte interamericana e della Corte europea dei diritti umani, è emersa una tendenza dei due organi giurisdizionali a riconoscere l'esercizio extraterritoriale della giurisdizione soltanto in casi eccezionali e principalmente sulla base del criterio del controllo effettivo sulle persone o sul territorio da parte delle truppe militari di uno Stato membro.

Infine, nel quinto e ultimo capitolo sono state presentate le proposte avanzate dai principali organi internazionali di controllo per tutelare in maniera più efficace il diritto alla protezione dei dati personali: la crittografia e l'anonimizzazione. Queste due tecniche

permettono, in un caso, di oscurare il contenuto di una conversazione e, nell'altro caso, di rendere impossibile l'identificazione del soggetto cui i dati personali si riferiscono.
In particolare, nel rapporto dello *Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression* pubblicato nel 2015 dallo *Special Rapporteur* Keyne, è stata dimostrata l'importanza della crittografia e dell'anonimizzazione per proteggere non solo il diritto alla privacy, ma anche altri importanti diritti fondanti qualsiasi società democratica come la libertà di espressione e religione.

In conclusione si può sostenere che, in mancanza di una soluzione univoca in merito ai diversi aspetti problematici analizzati nel corso del presente elaborato, sia sempre necessario ispirarsi al principio di proporzionalità, e agli altri principi sanciti nei diversi trattati internazionali ed europei che tutelano il diritto alla protezione dei dati personali, tutte le volte in cui si è chiamati a bilanciare, da un lato, le esigenze di tutela del singolo e, dall'altro lato, la necessità di preservare la sicurezza pubblica e di permettere alle autorità di *law enforcement* di svolgere le proprie attività investigative. Solo in questo modo è possibile difendere l'essenza dei diritti umani e preservare lo stato di diritto proprio di qualsiasi società democratica. Emblematica al riguardo è l'affermazione di Edward Snowden, evocata dal giudice Dedov nella sua opinione concorrente relativa al caso *Roman Zakarov c. Russia*, secondo cui "With each court victory, with every change in the law, we demonstrate facts are more convincing than fear. As a society, we rediscover that the value of the right is not in what it hides, but in what it protects".

BIBLIOGRAFIA

- ANRÒ, *Il margine di apprezzamento nella giurisprudenza della Corte di giustizia dell'Unione europea e della Corte europea dei Diritti dell'Uomo,* in *La funzione giurisdizionale nell'ordinamento internazionale e nell'ordinamento comunitario: atti dell'Incontro di studio tra i giovani cultori delle materie internazionalistiche, 7. edizione, Torino 9-10 ottobre 2009* (a cura di) A. ODENNINO, E. RUOZZI, A. VITERBO, F. COSTAMAGNA, L. MOLA, L. POLI, Napoli 2010.
- Y. ARAI-TAKAHASHI e altri, *Theory and Practise of the European Convention on Human Rights*, Intersentia, New York 2006
- Y. ARAI-TAKAHASHI, *The margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR,* Intersentia New York 2003
- I. BANTEKAS, L. OETTE, *International Human Rights Law and Practice*, Cambridge University Press, Cambridge 2013
- J.F. BARRETT, *Convergence, Compatibility or Decoration: The Luxembourg Court's References to Strasbourg Case Law in its Final Judgments*, in *Pécs Journal of International and European Law* 2016
- L. BARTELS, *The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects,* in *European Journal of International Law* 2015
- S. BARTOLE, P. DE SENA, V. ZAGREBELSKY (a cura di), *Commentario breve alla Convenzione europea per la tutela dei diritti dell'uomo e delle libertà fondamentali*, CEDAM, Padova 2012
- M. BASSINI, O. POLLICINO, *La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, in *La protezione transnazionale dei dati personali*, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, Roma TrE-PRESS, Roma 2016
- E. BENVENISTI, *Margin of appreciation, consensus, and universal standards*, in *Journal of International Law and Politics* 1999
- S. BESSON, *The Extraterritoriality of the European Convention on Human Rights: Why Human Rights Depend on Jurisdiction and What Jurisdiction Amount to,* in *Leiden Journal of International Law* 2012
- F. BIGNAMI, *Privacy and Law Enforcement in the European Union: The Data Retention Directive,* in *Chicago Journal of International Law* 2007

- E. BLACK, *L'IBM e l'olocausto*, traduzione a cura di R. ZUPPET e S. MANCINI, Rizzoli, Milano 2001
- A. BLASI, *La protezione dei dati personali nella giurisprudenza della Corte europea dei diritti dell'uomo*, in *Rivista Internazionale dei diritti dell'Uomo* 1999
- F. BOEHM, P. DE HERT, *Notification, an important safeguard against the improper use of surveillance - finally recognized in case law and EU law*, in *European Journal of Law and Technology* 2012
- F. BOEHM, *Assessing the New Instruments in EU-US Data Protection Law*, in *European Data Protection Law Review* 2016
- F. BOEHM, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice,* Springer 2012
- F. BOEHM, *Information Sharing in the Area of Freedom, Security and Justice – Towards a Common Standard for Data Exchange Between Agencies and EU Information System*, in S. GUTWIRTH, R. LEENES, P. DE HERT, Y. POULLET, *European Data Protection: In Good Health?*, Springer 2012
- F. BOEHM, *Data processing and law enforcement access to information systems at EU level*, *No consistent framework in spite of the envisaged data protection reform*, in *Datenschutz and Datensicherheit* 2012
- M. BONFANTI, *Cyber-security e privacy: la promozione della sicurezza nello spazio cibernetico attraverso la tutela della vita private e la protezione dei dati personali* in U. Gori S. Lisi (a cura di), *Information warfare 2015 Manovre cibernetiche: impatto sulla sicurezza nazionale*, Milano, 2016
- L. A. BYGRAVE, *International Agreements to protect personal data, in Global Privacy Protection*, edited by James B. Rule, Edward Elgar Publishing 2008
- I. BUFFARD, K. ZEMANEK: *The "Object and Purpose" of a Treaty: an Enigma?,* in *Austrian Review of International EE European Law* 1998
- L. BURGORGUE-LARSEN, *La Convention européenne des droits de l'homme*, LGDJ-Lextenso éditions, Issy-les-Moulineaux 2015
- I. CAMERON, *An introduction to the European Convention on Human Rights*, Iustus, Uppsala 2014
- F. CAPOTORTI, *Studio introduttivo*, in *Patti internazionali sui diritti dell'uomo*, in volume SIOI Padova 1967

- S. M. CARBONE, R. LUZZATTO, A.SANTA MARIA, *Istituzioni di diritto internazionale*, Giappichelli, Torino 2016
- M. M. CARUANA, *The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement*, in *International Review of Law, Computers & Technology* 2017
- C. CASTETS-RENARD, *Quelle Protection des Données Personnelles en Europe*? Larcier 2015
- D. CASTRO e R. ATKINSON, *Beyond Internet Universalism: A framework for Addressing Cross-Border Internet Policy*, The Information Technology & Innovation Foundation, Settembre 2014, disponibile alla pagina http://www2.itif.org/2014-crossborder-internet-policy.pdf
- N. CATELAN, S. CIMAMONTI, J.B. PERRIER*, La lutte contre le terrorisme dans le droit et la jurisprudence de l'Union européenne,* Presses Universitaire d'Aix- Marseille 2014
- C. M. CERNA, *Regional human rights systems*, Routledge, Londra 2014
- G. COEHEN, *La Convention européenne des droits de l'homme*, in *Revue Internationale de Droit Comparé* 1989
- J. CHRISTOFFERSEN, *Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights*, Martenus Nijhoff Publishers, Olanda 2009
- A. CILLI, *Manuale del Web, tecnologie, normative e management,* Franco Angeli, Milano 2004
- M. D. COLE, A. VANDENDRIESSCHE, *From Digital Rights Irland and Schrems in Luxembourg to Zakharov and Szabó/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance*, in *European Data Protection Law Review* 2016
- B. CONFORTI*, Diritto internazionale*, Editoriale Scientifica, Napoli 2018
- P. CZECH, *Überwachungsbefugnisse der Sicherheitsbehörden zur Terrorabwehr ohne richterliche Kontrolle,* in *Newsletter Menschenrechte* 2016
- J. D'ASPREMONT, A. NOLLKAEMPER, I. PLAKOKEFALOS, C. RYNGAERT, *Sharing Responsibility Between Non-State Actors and States in International Law: Introduction,* in *Netherlands International Law Review* 2015
- DAN JERKER B. SVANTESSON, *The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses,* in *Stanford Journal of International Law* 2014

- DAN JERKER B. SVANTESSON, *A new legal framework for the age of cloud computing*, disponibile alla pagina https://theconversation.com/a-new-legal-framework-for-the-age-of-cloud-computing-37055
- S. DAVIDSON, *The Civil and Political Rights Protected in the Inter-American Human Rights System*, in D. J. HARRIS, S. LIVINGSTONE, *The Inter-american System of Human Rights,* Oxford University Press 1998
- E. DE BUSSER, *EU data protection in transatlantic cooperation in criminal matters. Will the EU be serving its citizens an American meal?,* in *Utrecht Law Review* 2010
- P. DE HERT, V. PAPAKONSTANTINOU, *The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition*, in *Computer Law and Security Review* 2014
- F. DE LONDRAS, *Privatized counter-terrorist surveillance*, in F. DAVIS, N. MC. GARRITY, G. WILLIAMS, *Surveillance, Counter-Terrorism and Comparative Constitutionalism*, Routledge, Londra 2013
- M. DE SALVIA, *La Convenzione europea dei diritti dell'uomo*, Editoriale Scientifica, Napoli 2011
- M. DE SALVIA, *Lineamenti di diritto europeo dei diritti dell'uomo*, CEDAM, Padova 1992
- M. DE SALVIA, *Compendium de la CEDH. Les principes directeurs de la jurisprudence relative à la Convention européenne des droits de l'homme*, Editions N.P. Engel, Khel-Strasbourg-Arlington 1998
- P. DE SENA, *Proportionality and human rights in international law: some…"utilitarian" reflections*, in *Rivista di diritto internazionale* 2016
- O. DE SCHUTTER, *International Human Rights Law. Cases, Materials*, Commentary, Cambridge University Press 2014
- C. DE TERWANGNE, *The Work of Revision of the Council of Europe Convention 108 for the protection of Individuals as Regards the Automatic Processing of Personal Data*, in *International Review of Law, Computers & Technology* 2014
- M. DENNIS, *Application of Human Rights Treaties Extraterritoriality During Times of Armed Conflict and Military Occupation,* in Proceedings of the Annual Meeting (American Society of International Law), 2006
- S. DETRICK, *A commentary on the United Nations Convention on the Rights of the Child*, Martinus Nijhoff Publishers, Olanda 1999

- S. DETRICK, *The United Convention on the Rights of the Child*, a Guide to the "Travaux Préparatoires", Martinus Nijhoff Publishers, Olanda 1992
- F. DI MATTEO, *La raccolta indiscriminata e generalizzata di dati personali: un vizio congenito nella direttiva PNR*? In *Diritti umani e diritto internazionale* 2017
- D. DOERR, R. L. WEAVER, *Perspective on Privacy, increasing Regulation in the Usa, Canada, Australia and European Countries*, De Gruyter, Berlin/Boston 2014
- L. K. DONOHUE, *The Dawn of Social Intelligence (SOCINT*), in *Drake Law Review*, 2015
- S. DOTHAN, *Margin of Appreciation and Democracy: Human Rights and Deference to Political Bodies*, in *Journal of International Dispute Settlement* 2018
- C. DOYLE, M. BAGARIC, *The Right to privacy: Appealing, but Flawed,* in *International Journal of Human Rights* 2005
- K. DZEHTSIAROU, *European Consensus and the Evolutive Interpretation of the ECHR*, in *German Law Journal* 2011.
- N. EMILIOU, *The Principle of Proportionality in European Law*: a comparative Study, Kluwer Law International 1996
- M. FEINBERG, *International counterterrorism – national security and human rights: conflicts of norms or check and balances?,* In *The International Journal of Human Rights* 2015
- M.R. FERRARESE, *Il diritto orizzontale. L'ordinamento giuridico globale secondo Sabino Cassese,* in *Politica del diritto* 2007
- G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, in *La protezione transnazionale dei dati personali*, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, Roma TrE-PRESS, Roma 2016
- J. F. FLAUSS, DE SALVIA M. (a cura di), *La Convention européenne des droits de l'homme: développements récents et nouveaux défis*, Némésis-Bruylant, Bruxelles 1997
- M. FRANCHI, I. VIARENGO, *Tutela Internazionale dei Diritti Umani, Casi e materiali,* Giappichelli, Torino 2016
- A. FREIHERR VON DEM BUSSCHE, M. STAMM, *Data Protection in Germany,* Verlag C.H. Beck, Monaco 2013
- T.L. FRIEDMAN, *Il mondo è piatto*. *Breve storia del ventunesimo secolo,* Mondadori, Milano 2006
- C. FOCARELLI, *La persona umana nel diritto internazionale*, il Mulino, Bologna 2013
- L. FUMAGALLI, M. MERAVIGLIA, *Compliance Review nel Consiglio d'Europa*, Giuffrè, Milano 2004

- F. FONTANELLI, *The mythology of Proportionality in Judgements of the Court of Justice of the European Union on Internet and Fundamental Rights*, in *Oxford Journal of Legal Studies* 2016
- R. Z. GEORGE, H. RISHIKOF, *National Security Enterprise: Navigating the Labyrinth*, Georgetown University Press 2017
- I. GEORGIEVA, *The right to privacy under fire – Foreign Surveillance under the NSA and the GCHQ and its compatibility with Art. 17 ICCPR and Art. 8 ECHR,* in *Utrecht Journal of International and European Law* 2015
- K. GORMLEY, *One Hundred Years of Privacy,* in *Wiscousin Law Review* 1992
- C. GRABENWATER, *European Convention on Human Rights: commentary*, Verlag C.H. Beck, Monaco 2014
- C. GRAZIANI, *PNR EU-Canada, la Corte di Giustizia blocca l'accordo: tra difesa dei diritti umani e implicazioni istituzionali*, in *DPCE on line* 2017
- G. GREENLEAF*, Renewing Convention 108: The CoE's 'GDPR Lite' Initiatives, in Privacy Laws & Business International Report* 2016
- S. GREER, *The margin of appreciation: interpretation and discretion under the European Convention on Human rights*, Council of Europe Publishing 2000
- S. GUTWIRTH, R. LEENES, P. DE HERT, *Reforming European Data Protection Law,* Springer 2015
- S. GUTWIRTH, Y. POULLET, P. DE HERT, *Data Protection in a Profiled World,* Springer 2010
- T.I. HARBO, *The Function of the Proportionality Principle in EU Law*, in *European Law Journal* 2010
- D.J. HARRIS, M. O'BOYLE, C. WARBRICK, *Law of the European Convention on Human Rights*, Oxford University Press 2014
- L. HENNEBEL, *La jurisprudence du Comité des droits de l'homme des Nations Unies : le Pacte international relatif aux droits civils et politiques et son mécanisme de protection individuelle*, Bruylant, Bruxelles 2007
- R. HIGGINS, *Derogations under Human Rights Treaties,* in *British Yearbook of International Law* 1976-1977
- H. HIJMANS, *The European Union as Guardian of Internet Privacy*, Springer International 2016

- M. HILDEBRAND, *Profiling and AML*, in *The Future of Identity in the Information Society, Challenges and Opportunities*, ed. K. RANNENBERG, D. ROYER e A. DEUKER, Springer 2009
- S. H. HOFSTADTER, G. HOROWITZ, *The right of privacy*, Central Book Company, New York 1964
- J. C. HUTCHESON, *Law enforcement*, in *Central Law Journal* 1922
- D. IRELAND-PIPER, *Accountability in Extraterritoriality*, *A comparative and International Law perspective*, Edward Elgar Publishing 2017
- K. IRION, *A Special Regard: The Court of Justice and the fundamental rights to privacy and data protection,* in U. FABER, K. FELDHOFF, K. NEBE, K. SCHMIDT, U. WASSER (HRSG), *Gesellschaftliche Bewegugen-Recht unter Beobachtung und in Aktion,* Nomes, Baden Baden 2016.
- C. JASSERAND, *Law enforcement access to personal data originally collected by private parties: Missing data subject's safeguard in directive 2016/680?*, in *Computer Law & Security Law* 2018
- F. JIZENG, *Rethinking the Method and Function of Proportionality Test in the European Court of Human Rights,* in *The Journal of Human Rights* 2016
- M. G. JOHNSON, J. SYMONIDES, *The Universal Declaration of Human Rights, A history of its creation and implementation* 1948-1998, UNESCO Publishing 1998
- S. JOSEPH, M. CASTAN, *The International Covenant on Civil and Political Rights: cases, materials, and commentary*, Oxford University Press 2013
- D. JOYCE, *Internet Freedom and Human Rights,* in *The European Journal of International* 2015
- H. KELSEN, U. CAMPAGNOLO*, Diritto internazionale e lo Stato sovrano,* Giuffré, Milano 1999
- U. KILKELLY, *The right to respect for private and family life. A guide to the implementation of Article 8 of the European Convention on Human Rights*, Human Rights Handbooks. N. 01, Strasburgo 2003
- U. KOHL, *Jurisdiction and the Internet*, *Regulatory Competence over Online Activity*, Cambridge University Press 2007
- J. KOKOTT, C. SOBOTTA, *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*, in *International Data Privacy Law* 2017

- J. KRATOCHVIL, *The Inflation of the Margin of Appreciation by the European Court of Human Rights*, in *Netherlands Quarterly of Human Rights* 2011
- C. KUNER, *Internet Jurisdiction and Data Protection Law: An International Legal Analysis*, in *International Journal of Law and Information Technology* 2010
- H. LAUTERPACHT, *International Law and Human Rights*, Stevens & Sons Ltd, Londra 1950
- E. LAWSON, *Encyclopedia of Human Rights,* Taylor &Francis, Washington DC 1996
- Y LECUYER, *Convention européenne des droits de l'homme : les points clés de la protection des droits de l'homme par la Cour européenne des droits de l'homme*, Gualino-Lextenso éditions, Parigi 2015-2016
- A. LEGG, *The Margin of Appreciation in International Human Rights Law:Deference and Proportionality*, in *Human Rights Law Review* 2013
- G. LETSAS, *Two concepts of the margin of appreciation*, in *Oxford Journal of Legal Studies* 2006
- L. LORELLO, *Il dilemma sicurezza vs. libertà al tempo del terrorismo, Democrazia e Sicurezza*, in *Democracy and Security Review* 2017
- D. LOWE, *The European Union Passenger Name Record Data Directive: Is is Fit for Purpose?*, in *International Law Criminal Review* 2017
- N. LUBELL, *Extraterritorial Use of Force Against Non-State Actors,* Oxford University Press 2010
- R. LUZZATTO, *Stati stranieri e giurisdizione nazionale*, Giuffré, Milano 1972
- S. MACEDO, *Universal Jurisdiction, National Courts and the Prosecution of Serious Crimes under International Law,* University of Pennsylvania Press 2004
- P. MAHONEY, F. MATCHER, H. PETZOLD, L. WILDHABER, *Protection des droits de l'homme: la perspective européenne*, Carl Heymanns Verlag KG-Koeln-Berlin-Bonn-Muenchen, Colonia 2000
- V. MANTOUVALOU, *Extending Judicial Control in International Law: Human Rights Treaties and Extraterritoriality*, in *The International Journal of Human Rights* 2011
- F. MARTINES, *La Protezione degli Individui rispetto al trattamento automatizzato dei dati nel diritto dell'Unione Europea*, in *Rivista Italiana Diritto Pubblico Comunitario* 2000
- D. MCGOLDRICK, A *defense of the margin of Appreciation and an argument for its application by the Human Rights Committee*, in *International and Comparative Law Quarterly* 2016

- M. MILANOVIC, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, in *Harvard International Law Journal* 2015
- M. MILANOVIC, *Extraterritorial application of human rights treaties: Law, principles and policy,* Oxford University Press 2011
- A. R. MILLER, *The assault on privacy: computers, data banks, and dossiers,* The University of Michigan Press 1971
- S. MILLER, *Revisiting Extraterritorial Jurisdiction: A Territorial Justification for Extraterritorial Jurisdiction under the European Convention,* in *The European Journal of International Law* 2010
- P.-Y MONJAL, *Les dossier européens: actualités en bref, Protection des données à caractère personnel (la protection des personnes physiques à l'égard du traitement des données à caractère personnel: le règlement (UE) 2016/679 et la directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016,* in *Revue du droit de l'Union européenne* 2016
- L. MONTANARI, *I diritti dell'uomo nell'area europea tra fonti internazionali e fonti interne*, Giappichelli, Torino 2002
- A. MOWBRAY*, European Convention on Human Rights*, Oxford University Press 2012
- A. MOWBRAY, *Cases, Materials, and Commentary on the European Convention on Human Rights*, Oxford University Press 2010
- C. C. MURPHY, *EU Counter-Terrorism Law: Pre-Emption and the Rule of Law*, Hart Publishing 2015
- M. H. MURPHY*, Surveillance and the Right to Privacy: Is an "Effective Remedy" possible?, in Justiciability of Human Rights Law in Domestic Jurisdictions*, Edited by A. DIVER and J. MILLER, Springer 2016
- B. NASCIMBENE (a cura di), *La Convenzione europea dei diritti dell'uomo. Profili ed effetti nell'ordinamento italiano*, Giuffrè, Milano 2002
- M. NINO, *Il caso "Datagate":i problemi di compatibilità del programma di sorveglianza PRISM con la normativa europea sulla protezione dei dati personali e della privacy*, in *Diritti Umani e Diritto Internazionale* 2013
- M. NINO, *Terrorismo Internazionale, privacy e protezione dei dati personali*, Editoriale Scientifica, Napoli 2012
- M. NOWAK, *U.N. Covenant on Civil and Political Rights*, CCPR COMMENTARY, N.P. Engel publisher 2005

- M. O'BOYLE, *Emergency Government and Derogation under the ECHR,* in *European Human Rights Law Review* 2016
- M. OROFINO, *FBI v. Apple: il caso è (forse) chiuso, ma le questioni di fondo rimangono apertissime,* in *DPCE online* 2016
- R. C. OWENS, *Human Rights and the Internet, Balance and exercise of fundamental rights online,* in *Computer Law Review* 2008
- F. PAEFGEN, *Der von Art. 8 EMRK gewährleistete Schutz von staatlichen Eingriffen in die Persönlichkeitsrechte im Internet*, Springer 2017
- M. PALMISANO, *The Surveillance Cold War: Recent Decisions of the European Court of Human Rights and their application to mass surveillance in the United States and Russia*, in *Gonzaga Journal of International Law* 2017
- M. PANEBIANCO*, Giurisdizione interna e immunità degli Stati stranieri,* Iovene, Napoli 1967
- F. PAOLOZZI, *Focus sulla giurisprudenza costituzionale in materia di pubblica sicurezza,* in Osservatorio Regionale 2011
- R. PARDOLESI, *Diritto alla riservatezza e circolazione dei dati personali*, Giuffrè, Milano 2003
- F. PATRONI GRIFFI, *The margin of appreciation in the European Court's case-law*, in *Rivista Italiana di Diritto Comunitario* 2015
- J. PERRY BARLOW, *A Declaration of the Independence of Cyberspace,* 8 febbraio 1996, disponibile alla pagina https://www.eff.org/it/cyberspace-independence
- S. PEYROU, *Un nouveau cadre juridique général pour la protection des données au sein de l'Union européenne : une réforme législative ambitieuse*, in *Revue des affaires européenne* 2012
- L. PINESCHI, *La tutela internazionale dei diritti umani, norme, garanzie, prassi,* Giuffré, Milano 2015
- F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali, Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, Torino 2016
- F. POCAR, *I Diritti Umani a 40 anni dalla Dichiarazione Universale,* CEDAM, Padova 1989
- O. POLLICINO, *Internet nella giurisprudenza delle Corti europee: prove di dialogo?,* in *Forum di Quaderni costituzionali*, 31 dicembre 2013

- M. G. PORCEDDA, *The Recrudescence of 'Security v. Privacy' after the 2015 Terrorist Attacks, and the Value of 'Privacy Rights' in the European Union*, in E. ORRÙ, M. G. PORCEDDA e S. WEYDNER-VOLKMANN, *Rethinking Surveillance and Control. Beyond the 'Securityversus Privacy' Debate*, Nomos, Baden Baden2017 (in corso di pubblicazione)
- M. POTO, *The Principle of Proportionality in Comparative Perspective*, in *German Law Journal* 2007
- T. PURVIS, *Human Rights and Security: reflection on an Integral Relation, in Human Rights Current Issues and Controversies*, Edited by Gordon Di Giacomo, North York, Ontario: University of Toronto Press 2016
- N. PURTOVA, *Between the GDPR and the Police Directive: navigating through the maze of information sharing in public-private partnerships,* in *International Data Privacy Law* 2018
- R. QUADRI*, Diritto Internazionale Pubblico,* Liguori Editore, Padova 1949
- T. QUINTEL, *Article 29 Data Protection Working Party Opinion on the Law Enforcement Directive*, in *European Data Protection Law Review* 2018
- B.G. RAMCHARAN, *Human Rights- Thirty years after the Universal Declaration*, Martinus Nijhoff Publishers 1979
- M. H. RANDALL, M. HOTTELIER, *Introduction aux droits de l'homme*, Éditions Yvon Blais, Zurigo 2014
- I. RASILLA DEL MORAL, *The increasingly marginal appreciation of the Margin of appreciation doctrine*, in *German law journal* 2006
- K. REID, *A practitioner's guide to the European Convention on Human Rights*, Sweet & Maxwell, Londra 2015
- G. RESTA, *La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE*, (a cura di) G. RESTA, V. ZENO-ZENCOVICH, Roma TrE-PRESS, Roma 2016
- K. RETZER, *Data Breach notification: The changing Landscape in the EU,* in *Computer Law Review* 2008
- L. REYDAMS, *Universal Jurisdiction*, Oxford Monographs in International Law, Oxford 2004
- A. RISTROPH, *Proportionality as a Principle of Limited Government*, in *Duke Law Journal* 2005
- Y. RONEN, *Big Brother's Little Helpers: The Right to privacy and the Responsibility of Internet Service Providers*, in *Utrecht Journal of International and European Law* 2015

- A. RUEDA, *The implications of Strong Encryption Technology on Money Laundering,*in *Albany Law Journal Of Science & Technology* 2001
- E. RUSEN, J. VELU, *Convention européenne des droits de l'homme*, Bruylant, Bruxelles 2014
- C. RUSSO, P. QUAINI, *La Convenzione europea dei diritti dell'uomo e la giurisprudenza della Corte di Strasburgo*, Giuffrè, Milano 2000
- K. SALCITO, M. WIELGA, *What does Human Rights Due Diligence for Business Relationships Really Look Like on the Ground?*, in *Business and Human Rights Journal* 2018
- V. SALVATORE, *La Corte di giustizia restituisce (temporaneamente) agli Stati membri la competenza a valutare l'adeguatezza del livello di protezione dei dati personali soggetti a trasferimento verso gli Stati Uniti,* in *Studi sull'integrazione europea* 2015
- W. A. SCHABAS, *The European Convention on Human Rights*, a commentary, Oxford University Press 2015
- M. SCHACHTER, *Informational and Decisional Privacy*, Carolina Academic Press 2003
- L. SCHEECK, *Solving Europe's Binary Human Rights Puzzle. The Interaction between Supranational Courts as a Parameter of European Governance*, Questions de Recherche / Research in Question N°15 – October 2005, disponibile alla pagina http://www.ceri-sciences-po.org/publica/qdr.htm.
- D. J. SHERWINTER, *Surveillance's slippery slope: using encryption to recapture privacy rights,* in *Journal on Telecommunication & High Technology Law* 2007
- M. SCHREMS, *The Privacy Shield is a Soft Update of the Safe Harbor*, in *European Data Protection Law Review* 2016
- D. SEVERSON, *American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change*, in *Harvard International Law Journal* 2015
- B. SIEMEN, *The EU-US Agreement on Passenger Name Records and EC-Law: Data Protection Competences and Human Rights Issues in International Agreement of the Community*, in *German Yearbook of International Law*, 2015
- M. SIMONCINI, *Risk Regulation Approach to EU Policy against Terrorism in the light of the ECJ/CFI jurisprudence*, in *German Law Journal* 2009
- R. SINGER, *Proportionate Thoughts About Proportionality,* in *Ohio State Journal of Criminal Law* 2010
- D. J. SOLOVE, *Nothing to Hide: The False Tradeoff Between Privacy and Security*, Yale University Press 2011

- S. SOTTIAUX*, Terrorism and the Limitations of Rights, the ECHR and the US Constitution,* Hart Publishing 2008
- G. SPERDUTI, *La Dichiarazione Universale dei Diritti dell'Uomo*, in *Comunità Internazionale* 1950
- M. J. STRAUSS, *Territorial Leasing in Diplomacy and International Law*, Brill Nijhoff, Leida 2005
- G. STROZZI, *Diritto dell'Unione europea*. *Parte speciale*, Giappichelli, Torino 2017
- P. TANZARELLA, *Il margine di apprezzamento*, in M. CARTABIA (a cura di), *I diritti in azione,* il Mulino, Bologna 2007
- A. TANZI*, Introduzione al diritto internazionale,* CEDAM, Padova 2010
- P. TAVERNIER, *Destin du Pacte international relatif aux droits civils et politiques vingt ans après son entrée en vigueur*, in MOURGEON J., Pouvoir et liberté, Bruylant, Bruxelles 1998
- M. TAYLOR, *The EU's human rights obligations in relation to its data protection law with its extraterritorial effect,* in *International Data Privacy Law* 2015
- M. TAYLOR, *Transatlantic Juridictional Conflicts in Data Protection Law, How the Fundamental Right to Data Protection Conditions the European Union's Exercise of Extraterritorial Jurisdiction,* GVO drukkers & vormgevers 2018
- C. TEITGEN-COLLY (ed.), *La Convention européenne des droits de l'homme, 60 ans et après?*, LGDJ- Lextenso éditions, Parigi 2013
- C. TOMUSHAT, *Human rights between idealism and pragmatism*, Oxford University Press 2014
- X. TRACOL*, "Invalidator" strikes back: The harbour has never been safe*, in *Computer Law and Security Review* 2016
- C. B. TRANBERG, *Proportionality and data protection in the case law of the European Court of Justice,* in *International Data Protection Law* 2011
- M. TUGENDHAT AND I. CHRISTIE, *The law of Privacy and the Media,* Oxford University Press 2013
- M. TZANOU, *Data Protection as a fundamental right next to privacy? Reconstructing' a not so new right*, in *International Data Privacy Law* 2016
- M. TZANOU, *The War Against Terror and Transatlantic Information Sharing: Spillovers of Privacy or Spillovers of Security?* in *Utrecht Journal of International and European Law* 2015

- M. TZANOU, *The EU as an emerging "Surveillance Society": The function creep case study and challenges to privacy and data protection,* in *Vienna Online Journal on International Constitutional Law* 2010
- B. VAN ALSENOY, *Reconciling the (extra)territorial reach of the GDPR with public international law,* in *Data Protection and Privacy under Pressure – Transatlantic tensions, EU surveillance, and big data,* Maklu 2017
- C. VAN DE HEYNING, *No place like home, Discretionary space for the domestic protection of fundamental rights*, in *Human Rights Protection in the European Legal Order: the interaction between the European and the National Courts*, edited by P. POPELIER, C. VAN DE HEYNING, P. VAN NUFFEL, Intersentia, Anversa 2011
- A. VEDASCHI, G. MARINO NOBERASCO, *From DRD to PNR: Looking for a New Balance Between Privacy and Security*, in D. COLE, F. FABBRINI, S. SCHULHOFER (eds.), *Surveillance, Privacy and Transatlantic Relations*, Hart Publishing, Oxford 2017
- M. J. VELU, *La Convention européenne des droits de l'homme et le droit au respect de la vie privée, du domicile et des communications*, in *Vie privée et droits de l'homme*, Bruylant-Bruxelles 1973
- G. VERHENNEMAN, F. COUDERT, *Widening and strengthening the appeal of Convention 108*, in *Data Protection Law & Policy* 2015
- I. VIARENGO, *Deroghe e restrizioni alla tutela dei diritti umani nei sistemi internazionali di garanzia*, in *Rivista di diritto internazionale* 2005
- S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy,* in *Harvard Law Review* 1890
- J.K. WEEKS, *Comparative Law of Privacy*, in *Clev. - Marshall Law Review* 1963
- N. WITZLEB, D. LINDSAY, M. PATERSON, S. RODRICK, *Emerging Challenges in Privacy Law,* Cambridge Intellectual Property and Information Law 2014
- R.C.A. WHITE, C. OVEY, B. RAINEY, E. WICKS, F.G. JACOBS, *European Convention on Human Rights*, Oxford University Press 2014
- P. L. ZANARDI, G. VENTURINI, *Crimini di guerra e competenze delle giurisdizioni straniere*, Giuffré, Milano 1998
- C. ZANGHÌ, *La protezione internazionale dei diritti dell'uomo*, Giappichelli, Torino 2013
- S. ZAPPALA', *L'universalità della giurisdizione e la Corte penale internazionale*, in Problemi attuali della giustizia penale internazionale, Il Mulino, Bologna 2005
- J. ZITTRAIN, *Be careful What you Ask for: Reconciling a Global Internet and a Local Law,* in Harvard Law School Public Law Research Paper 2003

SITI CONSULTATI

- https://www.garanteprivacy.it/documents/10160/10704/1707373
- https://transparency.twitter.com/en/information-requests.html
- https://transparency.oath.com/reports/government-data-requests.html
- https://transparencyreport.google.com/user-data/overview
- https://transparency.facebook.com/government-data-requests
- https://www.microsoft.com/en-us/about/corporate-responsibility/lerr/
- https://www.amnesty.org.nz/snapchat-skype-among-apps-not-protecting-users%E2%80%99-privacy
- https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf

ATTI E DOCUMENTI

Organi delle Nazioni Unite

- Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, 37esima sessione, 26 febbraio-23 marzo 2018, A/HRC/37/62
- Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy*, *Joseph A. Cannataci*, 34esima sessione, 27 febbraio-24 marzo 2017, A/HRC/34/60
- Consiglio per i diritti umani, *Report of the Special Rapporteur on the right to privacy,* 31esima sessione, 24 novembre 2016, A/HRC/31/64
- Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye,* 29esima sessione, 22 maggio 2015, A/HRC/29/32
- Consiglio per i diritti umani, *Report of the Office of the United Nations High Commissioner for Human Rights*, *The right to privacy in the digital age*, 27esima sessione, 30 giugno 2014, A/HRC/27/37
- Consiglio per i diritti umani, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, 23esima sessione, 17 Aprile 2013, A/HRC/23/40
- Consiglio per i diritti umani, *Guiding Principles on Business and Human Rights*, 27esima sessione, 6 luglio 2011, Risoluzione A/HRC/RES/17/4
- Commissione per i diritti umani (ora Consiglio per i diritti umani), *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while*

countering terrorism, Martin Scheinin, 62esima sessione, 23 dicembre 2005 E/CN.4/2006/98/Add.1

- Corte internazionale di giustizia, *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Parere consultivo, 9 luglio 2004, General list no. 131
- Comitato per i diritti umani, *General Comment no. 31*, *The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, 26 maggio 2004, CCPR/C/21/Rev.1/Add. 1326
- Comitato per i diritti umani, *General Comment no. 29, Article 4: Derogations during a State of Emergency*, 31 agosto 2001, CCPR/C/21/Rev1/Add11
- Commissione del diritto internazionale, *Responsibility of States for Internationally Wrongful Acts***,** in *Official Records of the General Assembly,* 56esima sessione*, Supplement No. 10* (A/56/10)
- Comitato per i diritti umani, *Comments on the United Republic of Tanzania*, 28 dicembre 1992, CCPR/C/79/Add.12
- Assemblea Generale delle Nazioni Unite, *Guidelines for the Regulation of Computerized Personal Data Files*, 14 dicembre 1990, Risoluzione n. 45/95
- Comitato per i diritti umani, *General Comment no. 16*: *Article 17 (Right to Privacy)*, 8 Aprile 1988, HRI/GEN/1/Rev. 9
- Assemblea Generale delle Nazioni Unite, *Declaration on the Use of Scientific and Technological Progress in the Interests of Peace and for the Benefit of Mankind*, 10 novembre 1975, Risoluzione n. 3384 (XXX)
- Proclamazione di Teheran, Final Act of the International Conference on Human Rights, Teheran, 22 aprile-13 maggio 1968, A/CONF. 32/41 at 3 (1968)
- Corte permanente di giustizia internazionale, *Francia c. Turchia, the S.S. Lotus Case,* sentenza del 7 settembre 1927, Serie A, n.10

<u>Organi e Agenzie dell'Unione europea</u>

- Article 29 Working Party (WP29), *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680),* il 29 Novembre 2017, 17/EN, WP 258
- Article 29 Working Party, *EU – U.S. Privacy Shield – First annual Joint Review*, 28 novembre 2017, 17/EN, WP 255
- *Communication from the Commission to European parliament, the European Council and the Council on the European Agenda on Security to fight against terrorism and pave the way*

towards an effective and genuine Security Union, Bruxelles, 20 aprile 2016 COM(2016) 230 final

- Report FRA (European Union Agency for Fundamental Rights) *Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Volume II: field perspectives and legal update*, ottobre 2017
- Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques*, 10 aprile 2015, 0829/14/EN WP216
- Garante europeo per la Protezione dei dati, *Sintesi del parere del Garante europeo della protezione dei dati sulla comunicazione della Commissione al Parlamento europeo e al Consiglio «Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA» e sulla comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime «Approdo sicuro» dal punto di vista dei cittadini dell'UE e delle aziende ivi stabilite*, 16 aprile 2014, 2014/C 116/04
- *Article 29 Working Party (WP29)*, *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 10 aprile 2014, 819/14/EN WP 215
- Relazione del Parlamento europeo sul programma di sorveglianza dell'Agenzia per la sicurezza nazionale degli Stati Uniti, sugl organi di sorveglianza in diversi Stati membri e sul loro impatto sui diritti fondamentali dei cittadini dell'UE, e sulla cooperazione transatlantica nel campo della giustizia e degli affari interni, 21 febbraio 2014, 2013/2188(INI)
- Comunicazione della Commissione al Parlamento europeo e al Consiglio sul funzionamento del regime "Approdo sicuro" dal punto di vista dei cittadini dell'UE e delle società ivi stabilite, Bruxelles 27 novembre 2013, COM/2013/847 final
- Comunicazione della Commissione al Parlamento europeo e al Consiglio "Ripristinare un clima di fiducia negli scambi di dati fra l'UE e gli USA", 27 novembre 2013, COM/2013/846 final
- Consiglio europeo, *Programma di Stoccolma, Un'Europa aperta e sicura al servizio e a tutela dei cittadini*, 4 maggio 2010, 2010/C 115/01
- Consiglio dell'Unione europea, *Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection*, 23 novembre 2009, doc. n. 15851/09 JAI 822 DATAPROTECT 74 USA 102
- U.S.- Europol Supplemental Agreement on the Exchange of Personal Data and Related Information (December 20, 2002) disponibile alla pagina https://www.state.gov/s/l/38629.htm

- Article 29 Working Party, *Working document on determining the international application of EU data protection law to personal ata processing on the Internet by non-EU based web sites*, 30 maggio 2002, 5035/01/EN/Final WP 56
- 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, 25 agosto 2000, GU L. 215/7

GIURISPRUDENZA

Corte europea dei diritti umani

- *Big Brother Watch e altri c. Regno Unito*, sentenza del 13 settembre 2018, ricorsi nn. 58170/13 e altri
- *Centrum För Rättvisa c. Svezia*, sentenza del 19 giugno 2018, ricorso n. 35252/08
- *Şahin Alpay c. Turchia*, sentenza del 20 marzo 2018, ricorso n. 16538/17
- *López Ribalda e altri c. Spagna*, sentenza del 9 gennaio 2018, ricorsi nn. 1874/13 e 8567/13
- *Sezgin Tanrikulu c. Turchia*, sentenza del 18 luglio 2017, ricorso n. 27473/06
- [GC] *Satakunnan Markkinapörssi Oy e Satamedia Oy c. Finlandia*, sentenza del 27 giugno 2017, ricorso n. 931/13
- *Szabo e Vissy c. Ungheria*, sentenza del 12 gennaio 2016, ricorso n. 37138/14
- [GC] *Roman Zakharov c. Russia*, sentenza del 4 dicembre 2015, ricorso n. 47143/06
- *Muna Macalin Moxamed Sed Dahir c. Svizzera*, sentenza del 15 settembre 2015, ricorso n. 12209/10
- *Pisari c. Repubblica di Moldavia e Russia*, sentenza del 21 aprile 2015, ricorso n. 42139/12
- *Y.Y. c. Turchia*, sentenza del 10 marzo 2015, ricorso n. 14793/08
- [GC] *Hassan c. Regno Unito,* sentenza del 16 settembre 2014, ricorso n.29750/09
- *L.H. c. Lettonia*, sentenza del 29 aprile 2014, ricorso n. 52019/07
- *Cusan e Fazzo c. Italia*, sentenza del 7 gennaio 2014, ricorso n. 77/07
- *Di Sarno e altri c. Italia,* sentenza del 10 gennaio 2012, ricorso n. 30765/08
- [GC] *L-Skeini e altri c. Regno Unito*, sentenza del 7 luglio 2011, ricorso n. 55721/07
- *Shimovolos c. Russia,* sentenza del 21 giugno 2011, ricorso n. 30194/09
- *Mosley c. Regno Unito*, sentenza del 10 maggio 2011, ricorso n. 48009/08
- *Losonci Rose e Rose c. Svizzera*, sentenza del 9 novembre 2010, ricorso n. 664/06

- *Schalk e Kopf c. Austria*, sentenza del 24 giugno 2010, ricorso n. 30141/04
- *Kennedy c. Regno Unito*, sentenza del 18 maggio 2010, ricorso n. 26839/05
- *Kemal Taskin e altri c. Turchia*, sentenza del 2 febbraio 2010, ricorsi nn. 30206/04 e altri
- [GC] *A. e altri c. Regno Unito,* sentenza del 19 febbraio 2009, ricorso n. 3455/05
- *Schlumpf c. Svizzera*, sentenza del 8 gennaio 2009, ricorso n. 29002/06
- [GC] *S. e Marper c. Regno Unito*, sentenza del 4 dicembre 2008, ricorsi nn. 30562/04 e 30566/04
- *Liberty e altri c. Regno Unito*, sentenza del 1 luglio 2008, ricorso n. 58243/00
- *Daróczy c. Ungheria*, sentenza del 1 luglio 2008, ricorso n. 44378/05
- *Case of the Association For European Integration And Human Rights And Ekimdzhiev c. Bulgaria,* sentenza del 28 giugno 2007, ricorso n. 62540/00
- *Pad e altri c. Turchia*, sentenza del 28 giugno 2007, ricorso n. 60167/00
- [GC] *Markovic e altri c. Italia*, sentenza del 14 dicembre 2006, ricorso n. 1398/03
- *Saddam Hussein c. Albania, Bulgaria, Croatia, Repubblica Ceca, Danimarca, Estonia, Ungheria, Islanda, Irlanda, Italia, Lituania, Paesi Bassi, Polonia, Portogallo, Romania, Slovacchia, Slovenia, Turchia, Ukraina e Regno Unito*, sentenza del 14 marzo 2006, ricorso n. 23276/04
- *Bilen c. Turchia*, sentenza del 21 febbraio 2006, ricorso n. 34482/97
- *Fadeyeva c. Russia*, sentenza del 9 giugno 2005, ricorso n. 55723/00
- *Abdülsamet Yaman c. Turchia*, sentenza del 2 novembre 2004, ricorso n. 32446/96
- *Yurttas c. Turchia*, sentenza del 27 maggio 2004, ricorsi nn. 25143/94 e 27098/95
- *Elçi e altri c. Turchia*, sentenza del 13 novembre 2003, ricorsi nn. 23145/93 e 25091/94
- *Christine Goodwin c. Regno Unito*, sentenza dell'11 luglio 2002, ricorso n. 28957/95
- [GC] *Bankovic e altri c. Belgio,* sentenza 19 dicembre 2001, ricorso n. 52207/99
- *Marshall c. Regno Unito*, sentenza del 10 luglio 2001, ricorso n. 41571/98
- [GC] *Cipro c. Turchia*, sentenza del 10 maggio 2001, ricorso n. 25781/94
- *Bensaid c. Regno Unito*, sentenza del 6 febbraio 2001, ricorso n. 44599/98
- *Rotaru c. Romania*, sentenza del 4 maggio 2000, ricorso n. 28341/95
- *Demir e altri c. Turchia*, sentenza del 23 settembre 1998, ricorso n. 71/1997/855/1062-1064
- *Guerra e altre c. Italia*, sentenza del 19 febbraio 1998, ricorsi nn. 116/1996/735/932
- *Aksoy c. Turchia*, sentenza del 18 dicembre 1996, ricorso n.100/1995/606/694
- *Tolstoy Miloslavsky c. Regno Unito*, sentenza del 13 luglio 1995, ricorso n. 18139/91

- *López Ostra c. Spagna,* sentenza del 9 dicembre 1994, ricorso n. 16798/90
- [Plenaria] *Brannigan e McBride c. Regno Unito*, sentenza del 26 maggio 1993, ricorsi nn. 14553/89 e 14554/89
- Commissione europea dei diritti umani, *Kerkhoven e Hinke c. Paesi Bassi*, sentenza del 19 maggio 1992, ricorso n. 15666/89
- *Kamasinski c. Austria*, sentenza del 19 dicembre 1989, ricorso n. 9783/1982
- [Plenaria] *Gaskin c. Regno Unito*, sentenza del 7 luglio 1989, ricorso n. 10454/83
- *Brogan e altri c. Regno Unito*, sentenza del 29 novembre 1988, ricorsi nn. 11209/84 e altri
- *Leander c.Svezia*, sentenza del 26 marzo 1987, ricorso n. 9248/81
- Commissione europea dei diritti umani, *S. c. Regno Unito*, sentenza del 14 maggio 1986, ricorso n. 11716/85
- Commissione europea dei diritti umani [Plenaria], *Mersch e altri c. Lussemburgo*, sentenza del 10 maggio 1985, ricorsi nn. 10439/83 e altri
- *X e Y c. Paesi Bassi*, sentenza del 26 marzo 1985, ricorso n. 8978/80
- *Malone c. Regno Unito*, sentenza del 2 agosto 1984, ricorso n. 8691/1979
- Commissione europea dei diritti umani, *Cipro c. Turchia*, rapporto del 4 ottobre 1983, ricorso n. 8007/77
- *Silver e altri c. Regno Unito*, sentenza del 25 marzo 1983, ricorsi nn. 5947/72 e altri
- *Marckx c. Belgio*, sentenza del 13 giugno 1979, ricorso n. 6833/74
- [Plenaria] *Sunday Times c. Regno Unito,* sentenza del 26 aprile 1979, ricorso n. 6538/74
- [Plenaria] *Klass e altri c. Germania*, sentenza del 6 settembre 1978, ricorso n. 5029/1971
- [Plenaria] *Irlanda c. Regno Unito*, 18 gennaio 1978, ricorso n. 5310/71
- *Handyside c. Regno Unito*, sentenza del 7 dicembre 1976, ricorso n. 5493/72
- Commissione europea dei diritti umani, *Danimarca, Norvegia, Svezia e Paesi Bassi c. Grecia* (il "caso Greco"), rapporto del 5 Novembre 1969, ricorsi nn. 3321/67 e altri
- *Caso Linguistico Belga (I)*, sentenza del 23 luglio 1968, ricorsi nn. 1474/62 e altri
- *Lawless c. Irlanda (n. 3),* sentenza del 1 luglio 1961, ricorso n. 332/57
- Commissione europea dei diritti umani, *Grecia c. Regno Unito*, rapporto del 26 settembre 1958, ricorso n. 176/56

Corte di giustizia dell'Unione europea

- [Grande Sezione], *Progetto di accordo tra il Canada e l'Unione europea – Trasferimento dei dati del codice di prenotazione dei passeggeri aerei dall'Unione al Canada*, 26 luglio 2017, parere n. 1/15
- [Grande Sezione], *Tele2 Sverige AB c. contro Post- och telestyrelsen e Secretary of State for the Home Department contro Tom Watson e altri*, sentenza del 21 dicembre 2016, cause riunite C-203/15 e C-698/15
- [Grande Sezione], *J.N. c. Staatssecretaris van Veiligheid en Justitie*, 15 febbraio 2016**,** C-601/15
- [Grande Sezione] *Maximilian Schrems c. Data Protection Commissioner, con l'intervento di:Digital Rights Ireland Ltd*, sentenza del 6 ottobre 2015, C-362/14
- [Seduta Plenaria] *Parere n. 2/13*, 18 dicembre 2014
- [Grande Sezione] *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, sentenza del 13 Maggio 2014, causa C-131/12
- [Grande Sezione] *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e a. e Kärntner Landesregierung* e altri, sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12
- *Commissione c. Ungheria*, sentenza del 6 novembre 2012, causa C-286/12
- [Grande Sezione] *Commissione c. Austria*, sentenza del 16 Ottobre 2012, causa C-614/10
- [Grande Sezione] *Air Transport Association of America e altri c. Secretary of State for Energy and Climate Change*, sentenza del 21 dicembre 2011, causa C-366/2010
- *Scarlet Extended SA c. Société belge des auteurs compositeurs et éditeurs (Sabam)*, sentenza del 24 novembre 2011, Causa C-70/10
- [Grande Sezione] *Volker e Markus Schecke GbR, Hartmut Eifert c. Land Hessen*, sentenza del 9 novembre 2010, cause riunite C-92/09 e C-93/09
- [Grande Sezione] *Commissione Europea c. The Bavarian Lager Co. Ltd*, sentenza del 29 giugno 2010, causa C-28/08 P
- *Frede Damgaard*, sentenza del 2 aprile 2009, C-421/2007
- [Grande Sezione] *Heinz Huber c. Germania*, sentenza del 16 Dicembre 2008, causa C-524/06
- [Grande Sezione] *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, sentenza del 29 gennaio 2008, C-275/06

- *Parlamento Europeo c. Consiglio dell'Unione europea e Parlamento europeo c. Commissione delle Comunità europee*, sentenza del 30 maggio 2006, cause riunite C-317/04 e C-318/04
- *Rechnungshof c. Österreichischer Rundfunk e altri e Christa Neukomm e Joseph Lauermann c. Österreichscher Rundfunk*, sentenza del 20 maggio 2003, cause riunite C-465/00, C-138/01 e C-139/01
- *Roquette Frères SA c. Directeur général de la concurrence, de la consommation et de la répression des fraudes*, con l'intervento della Commissione delle Comunità europee, sentenza del 22 ottobre 2002, C-94/00
- *Lisa Jacqueline Grant c. South-West Trains Ltd*, sentenza del 17 febbraio 1998, C-249/96
- *P. c. S. e Cornwall County Council,* sentenza del 30 aprile 1996, C-13/94
- *Hoechst AG c. Commissione delle Comunità europee*, sentenza del 21 settembre 1989, cause riunite C-46/87 e C-227/88
- *Cornelis Kramer e altri*, sentenza del 14 luglio 1976, cause reunite C-3, 4 e 6/76

<u>Commissione interamericana dei diritti umani e Corte interamericana dei diritti umani</u>

- Corte interamericana dei diritti umani, *Solicitada Por La República De Colombia Medio Ambiente Y Derechos Humanos*, 15 novembre 2017*,* Opinione consultiva Oc-23/17
- Commissione interamericana dei diritti umani, *Coard Et Al. c. Stati Uniti*, 29 settembre 1999, Rapporto n. 109/99
- Commissione inter-americana dei diritti umani, Case 11.589 Armando Alejandre Jr., Carlos Costa, Mario De La Peña, And Pablo Morales c. Cuba, 29 settembre 1999, Rapporto n. 86/99
- Commissione interamericana dei diritti umani, *Petition Victor Saldaño c. Argentina*, 11 marzo 1999, Rapporto n. 38/99
- Commissione inter-americana dei diritti umani, *Case 10.573 c. Stati Uniti*, 14 ottobre 1993, Rapporto n. 1/93 Del 14 Ottobre 1993