Dipartimento di Giurisprudenza

Cattedra di Diritto Costituzionale

L'evoluzione della protezione dei dati personali tra tecnologia, sicurezza nazionale e diritti fondamentali

RELATORE
Prof. Raffaele Bifulco

CANDIDATO
Francesco Maria Donnini
Matr. 116643

CORRELATORE
Prof. Gino Scaccia

ANNO ACCADEMICO 2016/2017

INDICE

Capitolo Primo

I Principi Costituzionali del Diritto alla Protezione dei Dati Personali

Sezione I

Diritto alla privacy e Diritto alla protezione dati

Sezione II

Le fonti europee sul diritto alla protezione dei dati personali

Capitolo Secondo

La Regolamentazione Europea sulla Protezione dei Dati Personali: dalla Direttiva 95/46/CE al nuovo Regolamento UE 2016/679

Sezione I

Una rapida panoramica degli interventi normativi dell'Unione europea dalla Direttiva 95/46/CE fino al nuovo Pacchetto della Protezione Dati

Sezione II

Le principali innovazioni introdotte dal Regolamento UE 2016/679

Capitolo Terzo

La protezione dei dati personali nell'ambito della pubblica sicurezza e della giustizia penale e le recenti applicazioni giurisprudenziali

Sezione I

La normativa europea di cooperazione giudiziaria e di polizia dalla Convenzione del Consiglio d'Europa fino alla Direttiva generale UE 2016/680

Sezione II

Le principali applicazioni giurisprudenziali tra istanze di sicurezza e tutela del diritto fondamentale alla protezione dei dati personali

INTRODUZIONE

La protezione dei dati personali è una tematica che, negli ultimi anni, ha assunto sempre più un'importanza centrale nel panorama giuridico, riverberando i propri riflessi anche sugli scenari economici, sociali e spesso politici di tutto il mondo.
Bisogna sottolineare fin da subito come ciò che spesso viene impropriamente e generalmente definito come *privacy*, non esaurisca completamente il concetto di protezione dati.
Se sicuramente possiamo affermare che la protezione dei dati personali sia funzionale alla protezione della *privacy* di un individuo, intesa come riservatezza e protezione di ciò che è privato, la protezione dei dati personali però è qualcosa di più specifico, un *quid pluris*, rispetto ai concetti di protezione della vita privata e familiare, del proprio domicilio e della corrispondenza, così come sancito dall'articolo 8 CEDU.
Il diritto alla protezione dei dati personali, semplicisticamente parlando, protegge i dati dell'individuo, intesi come quell'insieme di informazioni, afferenti a vari aspetti della vita di una persona (tanto della sua sfera privata, quanto della sua sfera sociale), che il soggetto decide di mettere a disposizione del "pubblico" o, al contrario, decide di non diffondere.
Il dato, allora, viene definito nella sua ultima "veste", come disegnata dal nuovo Regolamento UE 2016/679, come «*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)*», definendo identificabile «*la persona fisica che può essere identificata, direttamente o indirettamente, con particolare 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 della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*».
Inoltre, nel tempo, è cambiato il paradigma di tutela e la concezione stessa della protezione dei dati personali.

Da una concezione originaria prettamente "materiale" della protezione dati (come interpretata dal sistema di *common law* statunitense), che si rifà alla disciplina e alla tutela del diritto di proprietà, si è passati ad un'interpretazione più orientata alla visione della protezione dati come una declinazione dei diritti di libertà e di dignità della persona (così come intesa nel sistema continentale europeo).

I dati personali, dunque, non sono più concepiti come un qualcosa di cui il titolare ha il possesso materiale o la proprietà, bensì come l'insieme delle informazioni che, non solo, sono capaci di identificare una persona, ma che rappresentano l'essenza della personalità dell'individuo stesso, tanto nel suo aspetto privato, quanto in quello pubblico.

In poche parole è il patrimonio informativo che ci caratterizza come individui, la percezione che all'esterno gli altri hanno di noi.

Perciò è fondamentale che tale declinazione "informativa" della personalità si riconduca ai canoni tradizionali dei diritti di libertà, della dignità umana e del libero sviluppo della personalità, costituendo ciò che il *Bundesverfassungsgericht*, in una famosa sentenza del 1983, definì il principio dell'autodeterminazione informativa.

Autodeterminazione informativa che il Tribunale Costituzionale federale tedesco, coniuga proprio dalle due libertà fondamentali dello sviluppo della personalità e dell'intangibilità della dignità umana, definendola come il diritto dell'interessato a decidere in prima persona sulla cessione, l'uso e, più in generale, in merito a qualsiasi vicenda relativa ai dati che lo riguardano.

L'importanza di un dominio sul nostro patrimonio informativo, insieme ad una maggiore consapevolezza nell'impiego dei nostri dati personali in una "società digitale", risultano elementi essenziali al fine di proteggere il nucleo fondamentale delle libertà della persona, in un'epoca, come quella odierna, in cui l'utilizzo e lo scambio di informazioni per diverse finalità ha raggiunto il suo picco storico ed è destinato ad aumentare esponenzialmente.

Ciò in relazione, soprattutto, al contesto in cui il dato è calato: il trattamento e l'evoluzione delle tecnologie, a quest'ultimo, annesse e utilizzate.

Infatti la protezione dei dati personali, ancor prima del suo riconoscimento come diritto fondamentale ad opera della Carta di Nizza, si è sviluppata di pari passo (forse, bisogna ammettere, sempre alla rincorsa) con l'evoluzione tecnologica degli strumenti mediante i quali i dati personali venivano elaborati.

È infatti significativo il modo in cui la protezione dei dati personali nacque come risposta ai primi sistemi di elaborazione automatizzata dei dati.

Infatti i primi elaboratori automatizzati per l'analisi dei dati, ideati dalla compagnia americana IBM, furono utilizzati addirittura all'alba del secondo conflitto mondiale da parte dei regimi autoritari, che in tal modo erano capaci di esercitare un controllo generalizzato su tutta la popolazione, tramite la suddivisione della stessa in varie categorie, facilmente individuabili di volta in volta, al fine di attuare forme diverse di repressione politica, sociale, economica e razziale.

Invero, dalla comparsa dei primi sistemi di elaborazione automatizzata dei dati, che utilizzavano un sistema di lettura delle informazioni basata su schede perforate, la tecnologia ha fatto passi da gigante.

Infatti con l'avvento dell'era digitale e di tutte le sue principali innovazioni i diritti fondamentali di libertà e della dignità umana, affrontano sfide non meno gravi di quelle del passato.

In primis a causa dell'ingerenza, non poco rilevante, che queste tecnologie possono attuare nella vita di ogni persona, se esenti da un adeguato controllo e da sostanziali limiti.

Ciò soprattutto in relazione all'importanza economica che ha assunto lo scambio dei dati, a livello commerciale, tra le grandi imprese del nostro tempo che offrono servizi in rete (si pensi solamente ad aziende come Amazon, Ebay, Facebook, Google, Apple e Yahoo solo per citarne alcune).

In secundis (a parere di chi scrive, fattore non meno preoccupante) a causa della generale inconsapevolezza e leggerezza con il quale si acconsente a rendere

disponibili i nostri dati personali in cambio dell'utilizzo di applicazioni *smart* e servizi sempre più precisi e sofisticati. Sottovalutando come questa facile "resa" del nostro patrimonio informativo, la successiva circolazione e il trattamento dei nostri dati personali, possa influire negativamente sui vari aspetti della nostra quotidianità e delle nostre libertà.

Infatti i sistemi sempre più raffinati di *data analysis* e la realtà dei *big data*, permettono la raccolta e il trattamento di una quantità innumerevole di dati, per diverse finalità, in tempi brevissimi e con costi ridotti, che grazie all'utilizzo di procedimenti sempre più precisi, arrivano a ricavare "informazioni da informazioni" in misura potenzialmente infinita.

Inoltre l'evoluzione delle tecnologie legate all'*internet of things*, permettono di far comunicare diversi oggetti tra loro (come ad esempio uno smartphone e degli elettrodomestici) mediante l'utilizzo della rete, al fine di rendere sempre più efficienti e funzionali i servizi a disposizioni dell'essere umano.

Così facendo però, si permette la circolazione e la successiva proliferazione di dati personali capaci di raffigurare le preferenze, i gusti, le abitudini, le opinioni delle persone fino ad arrivare ad elaborare, con vari gradi di specificità, la previsione di condotte e comportamenti degli utenti; informazioni che verranno utilizzate da vari agenti e per finalità diverse su di un terreno evanescente, come quello della Rete, e in quanto tale difficilmente controllabile.

Dunque nella società digitale e delle tecnologie legate alle comunicazioni elettroniche, il diritto alla protezione dei dati personali risulta un valido presidio di tutti i diritti fondamentali.

Basti notare che nei principali strumenti normativi che disciplinano la protezione dei dati personali nei vari settori, dalla Direttiva 95/46/CE sino al nuovo Regolamento UE 2016/679, è sempre specificato che lo scopo e l'obiettivo principale è quello di proteggere «*i diritti fondamentali e le libertà delle persone, in particolare il diritto alla protezione dei dati personali*».

Quindi la protezione dei dati personali protegge un ampio spettro di situazioni che vanno dalla difesa degli individui da forme di controllo di massa, statale e

non; dall'elaborazione di profili in base alla raccolta di informazioni relative ai comportamenti e alle preferenze degli utenti della rete a scopi commerciali; nonché a tutela delle persone da forme di discriminazioni derivate dalla conoscenza dell'orientamento religioso, politico o sindacale, oppure in base all'origine razziale o etnica, o ancora, in base a dati che rivelino dettagli relativi allo stato di salute o alla vita sessuale degli individui, capaci di compromettere significativamente le sue relazioni private, quanto quelle sociali e professionali.

La tecnologia e il suo sviluppo è stato, fin dall'alba dei tempi, un innegabile fattore di costante miglioramento delle condizioni di vita dell'uomo e in quanto tale necessaria alla sua stessa evoluzione.

Nonostante ciò è necessario che al crescere dell'incisività della tecnologia in termini di lesione e limitazione dei diritti e delle libertà delle persone, siano garantite misure adeguate e rafforzate le posizioni di diritto esistenti.

Un'altra sfida capace di incidere fortemente sul diritto alla protezione dei dati personali, è rappresentata dalle recenti forme di terrorismo islamico, non solo per il fatto che siano capaci di utilizzare abilmente le nuove tecnologie (specialmente quelle delle *information communication technologies* e quelle informatiche) a scopo di propaganda, addestramento o per compiere direttamente *cyber crimes*, ma soprattutto per il clima emergenziale che portano con sé.

Clima emergenziale che, sull'onda emotiva dettata dalla paura, porta spesso alla creazione da parte degli Stati di normative eccezionali di contrasto che sacrificano, in nome della sicurezza nazionale, le tradizionali libertà e situazioni di diritto consolidato.

Anche in questo caso dunque risulta necessario un attento bilanciamento, da parte dei Legislatori e delle Corti in particolare, dei vari interessi in gioco, al fine di ottenere il risultato più efficiente possibile, tra la protezione di posizioni giuridiche imprescindibili, quali essenza del nostro essere soggetti di diritto, e l'esigenza della predisposizione di tutte le misure adeguate a garantire la sicurezza nazionale e il nostro stile di vita da attacchi esterni.

In questo lavoro di tesi, verrà analizzata la disciplina europea della protezione dei dati personali, generale e in tema di cooperazione nel settore di giustizia e polizia, valutando il rapporto e la diversa incidenza che, nel tempo, ha avuto sui sistemi dei diritti costituzionali tradizionali.

Nel primo capitolo verrà effettuata una panoramica storica della nascita e dell'evoluzione della protezione dei dati personali.
Partendo dal nucleo comune del *Right to privacy*, inteso prevalentemente come *the right to be let alone*, elaborato nel famoso articolo di Warren e Brandeis del 1890, si arriverà all'esperienza degli Stati totalitari dei primi del '900, che cambierà in modo significativo la percezione, anche se non in maniera immediata, dei due concetti sempre più distinti di riservatezza e protezione dei dati personali. Si procederà poi ad un'analisi delle principali fonti normative sovranazionali e nazionali (CEDU, Consiglio d'Europa, Unione Europea, Costituzioni e Legislazioni di settore degli Stati membri) che, dal secondo dopoguerra fino ai giorni nostri, hanno contribuito ad instillare il sentimento comune della necessità di una tutela di rango primario e costituzionale del patrimonio informativo di ogni persona, elevando il diritto alla protezione dei dati personali a diritto fondamentale per la difesa della libertà, della dignità e della personalità.

Nel secondo capitolo, ci si addentrerà più nello specifico nello studio dei principali strumenti normativi della materia.
Si analizzerà in primis l'importanza dei principi sanciti nella Direttiva 95/46/CE, che per molto tempo ha rappresentato la fonte fondamentale della protezione dei dati personali. Benché fosse esclusivamente una normativa di armonizzazione delle diverse legislazioni nazionali che si andavano formando nel settore, e in quanto tale non vincolante o direttamente applicabile, l'apparato generale ed elastico ha consentito, però, a questo strumento di fungere da abile "cassetta degli attrezzi", plasmandosi di volta in volta, nella forma più funzionale a

seconda della situazione che si trovava a fronteggiare, grazie soprattutto alla prodigiosa opera esegetica della Giurisprudenza e delle Autorità garanti.
Si passerà poi al raffronto con il nuovo Regolamento UE n. 679, introdotto nel 2016 con l'intento di aggiornare la disciplina rispetto all'evoluzione incessante della tecnologia nell'era digitale, a seguito dei comprovati limiti della Direttiva "Madre" del '95 (che bisogna ricordare, nacque in un momento storico in cui internet era al principio e ancora non aveva svelato le sue infinite potenzialità).
Si esamineranno le principali innovazioni apportate dal Regolamento e la capacità di elaborare soluzioni alle sfide poste dal contesto attuale. Anzitutto il fondamentale cambio di prospettiva e il passaggio da una forma di tutela a carattere successivo-riparatorio ad un'altra a carattere preventivo-precauzionale. Poi, in un secondo momento, si prenderanno in considerazione le modifiche al sistema previgente e l'introduzione di istituti inediti tra cui: i concetti di *privacy by design and privacy by default*, i nuovi diritti all'oblio e alla portabilità dei dati, gli istituti della valutazione d'impatto e la consultazione preventiva, le nuove regole sulla sicurezza del trattamento e sulla *data breach*, il nuovo regime di informativa, la nuova disciplina sul trasferimento dei dati personali verso Paesi terzi e l'introduzione di nuovi soggetti all'interno del panorama della protezione dati come il *Data protection officer* e l'Autorità di controllo Capofila.

Il terzo e ultimo capitolo, sarà incentrato sull'analisi della disciplina della protezione dei dati personali nel settore della cooperazione giudiziaria e di polizia.
Similmente a quanto fatto nel secondo capitolo, si cercherà di creare un ponte tra la vecchia disciplina e le novità apportate dalla nuova, racchiuse nella Direttiva UE 2016/680 (che insieme al Regolamento n. 679 formano il c.d. "Pacchetto protezione dati").
Successivamente si cercherà di analizzare l'annosa questione sui limiti che devono essere predisposti alle modalità di indagine e agli strumenti sempre più sofisticati (si pensi ai metodi di sorveglianza sempre più elaborati come nel caso

dei c.d. captatori informatici da remoto) utilizzati dalle autorità competenti ai fini della prevenzione e del contrasto a gravi reati e minacce, tra cui la sicurezza nazionale, anche in situazioni emergenziali come quella causata dal terrorismo internazionale.

Attraverso l'esame di alcune sentenze cardine, provenienti dalla giurisprudenza delle Corti sovranazionali (CEDU e Corte di Giustizia europea), nonché da quella delle Corti nazionali (*Bundesverfassungsgericht* e Corte di Cassazione italiana), si cercherà di estrapolare i principi base che, di volta in volta, consentono limitazioni più o meno estese ai diritti alla riservatezza e alla protezione dei dati personali. Si individueranno, infine, sempre grazie all'opera fondamentale della giurisprudenza in tema, le garanzie minime che devono essere riconosciute al fine di preservare il nocciolo duro dei diritti fondamentali della persona, anche qualora sia necessario operare e cooperare per difendere beni a carattere pubblicistico ritenuti prevalenti, come la sicurezza nazionale.

Capitolo I

I Principi Costituzionali del Diritto alla Protezione dei Dati Personali

Sezione I

Diritto alla Privacy e Diritto alla Protezione dati

1. Il concetto di Privacy come antenato della Protezione Dati

L'uomo fin dai tempi antichi ha convissuto con due sentimenti contrastanti.
Da un lato, un innato senso di associazionismo, quasi un istinto di sopravvivenza che lo ha portato a creare comunità, a relazionarsi, regolare, osservare e condividere timori, conoscenze, nuove scoperte, modi di vivere e di interpretare la vita stessa. Il necessario impulso di lasciare un segno nel mondo, testimonianza palpabile di una vita, un'impronta nella storia da condividere con chi presente, ma soprattutto con chi verrà dopo: in poche parole l'ambizione di voler essere ricordato e conosciuto.
Dall'altro lato, un geloso attaccamento a una dimensione dell' Io profondamente privata. Una proiezione intima che si riflette sulla realtà che lo circonda e si concretizza nei rapporti personali affettivi con familiari e amici, convinzioni e credenze religiose, nell'appartenenza ad un determinato gruppo etnico, a partire dai suoi costumi fino alle più semplici abitudini, esercitate tanto nella sfera morale quanto, al di fuori, nella sfera dimensionale rappresentata dalle quattro mura domestiche. Un patrimonio di sentimenti, idee, modi di essere e caratteri culturali strettamente legati all'identità stessa di una persona e che la definiscono in quanto tale.
Da ciò l'esigenza di creare uno schermo che risulti impermeabile agli attacchi esterni, capace di assicurare protezione a tutta quella gamma di informazioni riguardanti la vita di un individuo che si ritiene debbano rimanere relegate

all'interno della propria sfera personale o, volendo intenderla come costruzione negativa, non debbano essere necessariamente conosciute da altri.

Il concetto di diritto alla privacy, inteso come *the right to be let alone*, nasce a Boston il 15 dicembre 1890 ad opera di due giovani giuristi bostoniani Samuel D. Warren e Louis D. Brandeis.

Warren e Brandeis pubblicarono sull'*Harvard Law Review*, ancora una delle riviste di diritto più importanti negli Stati Uniti, il saggio *The Right to Privacy*[1] nel quale analizzavano in maniera approfondita le relazioni intercorrenti tra riservatezza da riconoscere ad un individuo, il diritto della stampa ad informare e al contempo quello dei cittadini ad essere informati.

Tratto unificante nella formazione tanto del concetto di privacy, quanto di quello della protezione dati, è lo sviluppo tecnologico[2]. Non a caso le dinamiche sociali che portarono i due giuristi americani all'elaborazione del loro articolo furono strettamente legate alla nascita di una nuova frontiera dell'informazione della stampa americana.

Warren e Brandeis scrivevano nelle prime righe del loro articolo: « *Recent inventions and business methods call attention to the next step which must be taken for the protection of the person… Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life…*».

Dunque i nuovi profili che andava ad assumere la stampa, proiettandosi in un'ottica commerciale, con strategia di impresa, erano i principali segnali d'allarme per il "sacro spazio della vita privata e domestica" dell'individuo. La capacità del giornalismo d'impresa di diffondere in maniera rapida e ampia una notizia, insieme ad un sempre maggiore utilizzo dello strumento fotografico a

[1] S.D. WARREN - L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, Vol IV, Boston 15 dicembre 1890, n.5. È possibile reperire il testo completo del saggio su www.groups.csail.mit.edu. Si veda inoltre J. Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity versus Liberty*, in *The Yale Law Journal*, New Haven (Connecticut), 2004.

[2] Lo sviluppo tecnologico, infatti, è un tema centrale nell'evoluzione del diritto alla *privacy* e alla protezione dei dati personali, nonché dei diritti in generale. A tal proposito ne fanno ampia analisi nei loro manuali, S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995 e F. PIZZETTI, *PRIVACY E IL DIRITTO EUROPEO ALLA PROTEZIONE DEI DATI PERSONALI-Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Torino, 2016.

supporto del contenuto scritto, ha fatto sì che anche fatti puramente mondani, fossero pietanza prelibata per l'insaziabile curiosità della borghesia bostoniana dell'ottocento.

Diventavano così di dominio pubblico (e si parlava già a quei tempi di decine di migliaia di lettori) fatti riguardanti non solo cittadini che non avevano specifiche responsabilità pubbliche, ma vicende che non avevano alcun tipo di rilevanza pubblica o comunque tali da giustificare gli ampi spazi dedicati dalle testate giornalistiche dell'epoca o un controllo così incessante.

In questo contesto, i numerosi articoli di cronaca riguardanti la vita privata di Warren e consorte sono stati, con molta probabilità, la causa scatenante da cui nacque la decisione di redigere l'articolo e che hanno indotto i due avvocati di Boston a cercare di elaborare e definire in modo concreto gli spazi ed i limiti tra riservatezza, libertà di stampa e libera manifestazione del pensiero, richiamando i diritti fondamentali enucleati nel *Bill of Rights* e, nello specifico, attraverso l'analisi del primo, quarto e quinto emendamento.

Rilevanti più del quinto emendamento[3], che apre i principi fondamentali del sistema di giustizia, sono il primo ed il quarto emendamento che congiuntamente rappresentano la vera *corner stone* dell'impianto sostanziale delle libertà del cittadino nei confronti dell'ingerenza dello Stato.

Il primo emendamento introduce le garanzie volte al riconoscimento delle libertà di culto, della manifestazione del pensiero dell'individuo in tutte le sue forme come singolo e come gruppo, la libertà di stampa e infine il diritto di ogni cittadino di associarsi liberamente.

Infine il quarto emendamento fissa il principio per cui nessuno può essere violato nella sua persona, casa ed effetti personali da perquisizioni, arresti e confische

[3] Il quinto emendamento infatti sancisce i punti cardine di ogni sistema processuale di uno Stato di Diritto: il divieto di essere perseguiti se non in forza di una formale accusa o una denuncia del *Grand Jury*; il principio di *ne bis in idem* per il quale nessuno può essere sottoposto due volte, per un medesimo fatto, a un procedimento che comprometta la sua vita o la sua integrità fisica; o ancora il divieto di *self incrimination* per il quale nessuno, in una causa penale, può essere obbligato a deporre contro sé stesso ovvero essere privato della propria vita, libertà, beni senza essere stato sottoposto precedentemente ad un giusto processo.

irragionevoli cioè non giustificate da adeguato mandato predisposto dall'autorità giudiziaria e con le dovute modalità richieste dalla legge.

È proprio da questi due emendamenti e dal catalogo delle garanzie che ne derivano che Warren e Brandeis cercarono di ritagliare uno spazio di tutela alla riservatezza della persona.

Bisogna dire da subito che l'intento dei due giuristi con la loro dissertazione non fu quello di erigere un nuovo diritto fondamentale autonomo, proponendo una modifica al testo costituzionale tramite il mezzo legislativo dell'emendamento, ma piuttosto quello della creazione della Privacy come un diritto che avesse una funzione di argine all'incontrollata espansione dei diritti presi in considerazione negli emendamenti primo e quarto, veri e propri capisaldi sui quali si fonda la Costituzione americana.

Dunque non risulta una volontà diretta alla parificazione tra diritto al *freedom of speech* e il *right to privacy*, ma piuttosto l'intenzione di elaborare un sistema di bilanciamento tra i due idoneo in concreto a tutelare la riservatezza della persona tramite la limitazione, nei casi consentiti, della libertà di stampa e di parola.

Ciò si evince espressamente proprio dal testo di *The Right to Privacy* nella parte in cui Warren e Brandeis tengono a specificare che *«The right to privacy does not prohibit any publication of matter which is of public or general interest»*, e cioè che il diritto alla riservatezza non proibisce la pubblicazione di alcun argomento di pubblico o generale interesse; oppure *«The right to privacy ceases upon the publication of the facts by the individual, or with his consent.»* nel senso per cui il diritto alla privacy non viene violato se la pubblicazione dei fatti, anche se di natura privata, avviene con il consenso della persona o per azione diretta della stessa.

È proprio da questi due incisi, che sembrano delimitare in negativo lo spazio riservato al diritto alla privacy, che in realtà estrapoliamo i veri e propri limiti all'ampiezza del diritto di stampa e dell'informazione pubblica nonché la vera e propria conformazione del diritto alla riservatezza come limite e barriera al "gossip" senza controllo della Boston ottocentesca.

Infatti sono due i criteri fondamentali da rispettare affinché la libera informazione non sia di ostacolo all'esercizio del diritto alla riservatezza di un individuo. Prima di tutto, la notizia deve riguardare fatti di pubblico interesse, perché chi coinvolto è un soggetto che riveste una qualifica pubblica e in quanto tale ha una responsabilità specifica nei confronti della collettività (si parla infatti in questi casi di privacy attenuata).

Infine il consenso rilasciato dal diretto interessato.

La preoccupazione principale di Warren e Brandeis era la mancanza all'interno del sistema di common law di una tutela legale effettiva dei sentimenti che, dall'intrusione e dalla curiosità altrui, subivano un "*injury"* inteso come vero e proprio danno suscettibile, secondo i due avvocati, di risarcimento.

Lamentavano, in modo specifico, che nel tempo la common law avesse sviluppato una protezione da ingerenze esclusivamente "fisica" che trovava nel diritto di proprietà, per analogia, la tutela più adeguata.

Privacy intesa cioè come *ius excludendi alios* dai confini della propria sfera privata.

Inquadrando, così, la privacy entro il "recinto" del rassicurante diritto di proprietà i sentimenti, i pensieri, le idee, le sensazioni diventavano parte integrante del supporto materiale nel quale si traducevano concretamente nella realtà: libri, composizioni musicali, statue, dipinti, lettere. In questo modo tutto il materiale, se reso pubblico dall'autore, poteva essere protetto per analogia dalle leggi sul diritto d'autore e dal diritto di proprietà.

Ma cosa accadeva nel caso mancasse la volontà del titolare di rendere pubbliche le proprie opere o quest'insieme di "*feelings"* non fosse stato trasposto su di un supporto materiale e venissero resi pubblici da altri tramite registrazioni sonore o fotografiche?

I due autori sottolineavano come il sistema di common law assicurasse a ciascun individuo il diritto di determinare fino a che punto i suoi pensieri, i sentimenti e le emozioni possano essere comunicati a terzi e rimarcavano come l'esistenza di

questo diritto fosse avulso dal particolare metodo di espressione adottata, che si trattasse della parola o di segni, di pittura, di scultura o musica.

Così facendo, la stessa protezione sarebbe dovuta essere stata accordata tanto ad una lettera informale o a una confidenza racchiusa in una voce di un diario privato, quanto a una poesia o un saggio di maggior pregio artistico.

In ciascuno di questi casi l'individuo ha il diritto di decidere se quello che è suo potrà essere consegnato al pubblico e nessun altro, senza il consenso del legittimo proprietario, ha il diritto di pubblicare le sue produzioni in qualsiasi forma.

I due giuristi americani tennero a chiarire che, affinché venisse riconosciuta una effettiva tutela ai sentimenti, era necessario ritagliare uno spazio in cui questo diritto fosse stato del tutto indipendente dal materiale su cui il pensiero, il sentimento o le emozioni sarebbero state espresse.

Allo stesso tempo si sottolineava l'esigenza che il *right to privacy* fosse del tutto sganciato dalle leggi sul copyright, il cui scopo principale è quello di garantire all'autore, compositore, artista la percezione nella sua interezza degli utili derivanti dal suo lavoro e che per operare necessitano di una pubblicazione.

Più volte la giurisprudenza americana ha ricondotto la tutela di queste situazioni nell'alveo del diritto di proprietà.

Gli stessi Warren e Brandeis in prima battuta, ammisero che le somiglianze non sono poche, specialmente se si ha riguardo alle composizioni letterarie o alle riproduzioni artistiche. Esse hanno molti degli attributi della *property* ordinaria: sono trasferibili, hanno un valore e la loro pubblicazione o riproduzione è un mezzo mediante il quale tale valore si realizza.

Proseguendo però nella loro analisi i due giuristi affermarono che, qualora non ci si soffermasse più sui profili inerenti la proprietà intellettuale legata all'opera, e si prendessero in considerazione la volontà del titolare di vietare la pubblicazione o impedire che venissero svelati dettagli, confidenze della sua vita privata al fine di tutelare quella che in un passo dell'articolo viene definita *"peace of mind"* (che tradotto letteralmente significa "pace della mente", ma che

personalmente mi sentirei di definire più come serenità interiore) la struttura del diritto di proprietà sembrava perdere d'efficacia.
Ricondurre sotto il concetto fin troppo "materiale" di proprietà questo bene giuridico risultava essere riduttivo, poiché i due avvocati americani sottolinearono come il bene tutelato non fosse tanto lo scritto contenente il fatto privato riportato, bensì il fatto in sé che l'individuo non voleva fosse diffuso.
Conclusero così affermando che la tutela accordata a pensieri, sentimenti ed emozioni, espressa per mezzo della scrittura e delle arti, per quanto essa possa consistere nel prevenire la pubblicazione, non era in realtà, altro che un esempio del più generale diritto dell'individuo di "essere lasciato da solo" e di conseguenza, il principio che proteggeva gli scritti personali e i fatti di vita privata dell'individuo, non contro il furto e l'appropriazione fisica, ma contro la pubblicazione in qualsiasi forma, era in realtà non il diritto a difesa della proprietà privata, ma quello dell'inviolabilità della persona.
Infine bisogna senz'altro concludere che la più grande intuizione dei due giuristi bostoniani nel redigere l'articolo *The Right to Privacy* è stata quella di spostare l'attenzione del panorama giuridico americano sulla vera dimensione del diritto alla riservatezza, inteso non più come estensione del diritto di proprietà, ma avente una dimensione strettamente individuale collegata alla personalità dell'individuo.

2. La protezione dei dati personali, nascita ed evoluzione attuale

Il diritto è una materia in costante evoluzione, mai statica. La sua essenza è malleabile e lo rende capace di adeguarsi alle dinamiche del tempo in cui vive. Allo stesso modo e con gli stessi ritmi con cui l'umanità cresce e sviluppa nuove tecnologie, nuovi modi di sentire i valori e affrontare le problematiche del suo tempo, il "buon" diritto segue le sue orme e vi si adegua. Il diritto si sviluppa per mezzo dell'uomo, l'uomo si evolve e nobilita per mezzo del diritto.

Abbiamo visto come nell'esperienza americana la *privacy* nasca quale diritto "di contrasto" per la borghesia americana contro l'ingerenza ingiustificata dei mezzi di informazione all'interno della sua dimensione privata[4]. La privacy si presenta dunque come la conquista di un privilegio borghese e ad esclusivo appannaggio della borghesia.

Si può certamente ricondurre sotto l'alveo del più ampio diritto alla riservatezza anche il concetto di protezione dei dati personali. Quest'ultimo, però, a ben vedere costituisce una specificazione del più generale diritto alla privacy. Dunque, la protezione dei dati personali si configurerebbe come *species* rispetto al *genus* riservatezza.

Fattore comune nella nascita di entrambi i diritti è stato senz'altro lo sviluppo tecnologico e l'evoluzione, nello specifico, dei mezzi di comunicazione. Se nell' America dell'ottocento la nuova sfida da affrontare per la privacy era rappresentata dalla stampa offset e dai nuovi metodi imprenditoriali del giornalismo, per la protezione dati i nuovi ostacoli alla tutela della libertà e della dignità delle persone sono stati, nell'Europa di inizio novecento, i nuovi sistemi di raccolta dei dati riguardanti ogni genere di informazione sulle persone e adesso, nell'epoca in cui viviamo, dai nuovi traguardi della società digitale, del *Web2.0*[5], dei *Big data*[6], dell'*Internet of Things*[7] (IoT) fino ad arrivare alle

---

[4] Si rimanda ancora a S.D. WARREN - L.D. BRANDEIS, *The Right to Privacy*, in *Harvard Law Review*, Vol IV, Boston 15 dicembre 1890, n.5.

[5] Il *Web 2.0* è un'espressione utilizzata per indicare uno stato dell'evoluzione del World Wide Web, rispetto a una condizione precedente. Si indica come Web 2.0 l'insieme di tutte quelle applicazioni online che permettono un elevato livello di interazione tra il sito web e l'utente come i blog, i forum, le chat, le piattaforme di condivisione di media come YouTube, i social network come Facebook, Myspace, Twitter. È definito "Web dinamico" in contrapposizione al cosiddetto "Web statico" o "Web 1.0", cioè senza alcuna possibilità di interazione con l'utente eccetto la normale navigazione ipertestuale tra le pagine, l'uso delle e-mail e dei motori di ricerca.

[6] Per *Big data* si intende un ingente insieme di dati digitali che possono essere rapidamente processati da banche dati centralizzate. L'immagine più suggestiva per comprendere Big Data la offre Dave Menninger di Greenplum: "Il pianeta è diventato un organismo vivente, che comunica continuamente e Internet ne rappresenta il sistema nervoso" e di cui i big data ne rappresentano gli infiniti impulsi nervosi ed informazioni. L. INDEMINI, *Stampa .it, 2012, Tecnologia,* in ENCICLOPEDIA TRECCANI ONLINE, www.treccani.it , definizione big data.

[7] *L'Internet delle Cose* (*IoT*, acronimo dell'inglese *Internet of Things*) è un neologismo introdotto da Kevin Ashton riferito all'estensione di Internet al mondo degli oggetti e dei luoghi concreti. Nell'Internet delle cose gli oggetti (le "cose") si rendono riconoscibili e acquisiscono intelligenza grazie al fatto di poter comunicare dati su se stessi e accedere ad informazioni aggregate da parte di altri. Le sveglie suonano prima in caso di traffico, le scarpe da ginnastica trasmettono tempi, velocità e distanza

ulteriori derivazioni costituite dalle piattaforme multimediali di comunicazione come i *social networks*[8] di cui il più celebre è Facebook e le applicazioni[9] per cellulari e smartphone di messaggistica istantanea[10] come Whatsapp e Telegram, solo per citarne alcune.

Per questi e altri motivi il diritto alla protezione dei dati personali si differenzia dal diritto alla riservatezza; esso ha avuto un percorso diverso tanto per il contesto spazio - temporale in cui nasce quanto per il bene giuridico tutelato.

Sotto il primo profilo, non può sottovalutarsi il percorso storico che hanno affrontato i paesi europei nella prima metà del XX secolo.

Senza inoltrarsi in un'approfondita analisi storica della diversa concezione del binomio Stato-Cittadino durante le varie epoche storiche, che partono dalla

---

per gareggiare in tempo reale con persone dall'altra parte del globo, i vasetti delle medicine avvisano i familiari se si dimentica di prendere il farmaco. Tutti gli oggetti possono acquisire un ruolo attivo grazie al collegamento alla Rete. L'obiettivo dell'internet delle cose è far sì che il mondo elettronico tracci una mappa di quello reale, dando un'identità elettronica alle cose e ai luoghi dell'ambiente fisico. Gli oggetti e i luoghi muniti di etichette Identificazione a radio frequenza (Rfid) o Codici QR comunicano informazioni in rete o a dispositivi mobili come i telefoni cellulari. I campi di applicabilità sono molteplici: dalle applicazioni industriali (processi produttivi), alla logistica e all'info-mobilità, fino all'efficienza energetica, all'assistenza remota e alla tutela ambientale. Per una semplice, ma pertinente analisi sul concetto dell'IoT vedi anche WIKIPEDIA, the free encyclopedia, *definizione Internet of Things.*

[8] *Social Network* è un'espressione *che* identifica un servizio informatico online che permette la realizzazione di reti sociali virtuali. Si tratta di siti internet o tecnologie che consentono agli utenti di condividere contenuti testuali, immagini, video e audio e di interagire tra loro. Generalmente i s. n. prevedono una registrazione mediante la creazione di un profilo personale protetto da password e la possibilità di effettuare ricerche nel database della struttura informatica per localizzare altri utenti e organizzarli in gruppi e liste di contatti. Le informazioni condivise variano da servizio a servizio e possono includere dati personali, sensibili (credo religioso, opinioni politiche, inclinazioni sessuali ecc.) e professionali. Sui s. n. gli utenti non sono solo fruitori, ma anche creatori di contenuti. La rete sociale diventa un ipertesto interattivo tramite cui diffondere pensieri, idee, link e contenuti multimediali. ENCICLOPEDIA TRECCANI ONLINE ,www.treccani.it, definizione *social network.*

[9] In informatica, *un'Applicazione Mobile* (nota anche con l'abbreviazione *app*) è un'applicazione software dedicata ai dispositivi di tipo mobile, quali smartphone o tablet. Una app per dispositivi mobili si differenzia dalle tradizionali applicazioni sia per il supporto con cui viene usata sia per la concezione che racchiude in sé. Si tratta a tutti gli effetti di un software che per struttura informatica è molto simile a una generica applicazione, ma è caratterizzata da una semplificazione ed eliminazione del superfluo, al fine di ottenere leggerezza, essenzialità e velocità, in linea con le limitate risorse hardware dei dispositivi mobili rispetto ai desktop computer. Le app così descritte si definiscono *native* perché create appositamente per uno specifico sistema operativo e ampliano le capacità native del dispositivo incluse all'interno del sistema operativo (configurazione di base).

[10] La *Messaggistica Istantanea* (in lingua inglese *instant messaging*) è una categoria di sistemi di comunicazione in tempo reale in rete, tipicamente Internet o una rete locale, che permette ai suoi utilizzatori lo scambio di brevi messaggi. Le differenze principali rispetto alla posta elettronica o altri tipi di chat sono non solo nella brevità dei messaggi o nella velocità della loro consegna, ma anche nel fatto che, il modello di comunicazione sia sincrona. I sistemi di messaggistica istantanea sono realizzati con architettura peer-to-peer, nella quale le applicazioni usate dagli utenti comunicano direttamente tra loro, o con quella client-server, dove invece le comunicazioni sono mediate da un servizio centrale.

Rivoluzione Francese sino all'epoca attuale, appare innegabile come i malumori, le crisi economiche, le disillusioni conseguenti al primo grande conflitto mondiale hanno aperto la strada al nascere di movimenti nazionalisti, che cavalcando il malessere del popolo, si sono proposti come soluzione ai problemi della società, tramite l'instaurazione di un potere forte, centrale e assoluto.

I regimi totalitari, nello specifico quello Nazista tedesco e quello Fascista italiano, erano caratterizzati da un forte accentramento dei poteri e il corollario della stabilità e della sopravvivenza dello Stato-Partito, tanto dagli attacchi esterni, quanto da quelli interni, era un incessante controllo sulla popolazione.

Ogni aspetto della vita di una persona era minuziosamente regolata fin dall'infanzia (si pensi alla Gioventù Balilla), ogni azione del cittadino doveva contribuire al florido sviluppo dello Stato Fascista/Nazista, anche il più piccolo degli atti quotidiani come fare la spesa era parte di un più alto dovere civico indirizzato in tal senso.

Di conseguenza, ogni comportamento deviante o che solamente facesse venire il sospetto di una qualche non conformità agli obblighi di vita fascista o nazista doveva essere rapidamente individuato e, altrettanto celermente, neutralizzato.

Ma qual era il meccanismo, la tecnica mediante la quale attuare questo controllo continuo e totale di massa?

Ancora una volta irrompe prepotentemente sulla scena, lo sviluppo tecnologico, come descrive il Professor Franco Pizzetti nella sua attentissima analisi storica delle dinamiche che portarono al riconoscimento, successivamente all'esperienza degli Stati Autoritari in Europa, di una sensibilità condivisa rispetto alla necessità di una protezione inerente i dati personali dell'individuo[11]. Egli afferma in proposito che «*Sul piano delle tecnologie che resero possibile le più pervasive forme di controllo globale, un posto centrale spetta infatti ai trattamenti*

[11] F. PIZZETTI, *Privacy e il Diritto...*, cit., p. 52 e ss.

automatizzati, basati in quel tempo essenzialmente sulle schede perforate[12] *e sui sistemi di elaborazione dati*[13] *messi a punto, per prima, dalla IBM*[14].».

Questi sistemi di elaborazione dati permettevano in tempi rapidissimi l'acquisizione, l'archiviazione, l'analisi ed il trattamento di un'innumerevole mole di informazioni riguardanti ogni aspetto della vita di una persona.

Inoltre la raccolta e il trattamento dei dati avvenivano senza alcun criterio predeterminato in merito a specifiche finalità, come ad esempio la ricerca di informazioni concernenti la commissione di un fatto-reato, consentendo tecniche di conservazione generalizzate di qualsiasi dato e su qualsiasi cittadino.

La raccolta così descritta di tali informazioni non era attuata da questi regimi solamente al fine di garantire la stabilità e la sicurezza del potere, tramite il controllo dei propri cittadini, ma spesso risultava essere un abile strumento attraverso il quale attuare quelli che erano i piani di propaganda e ideologici di partito.

Le disumane conseguenze del disegno nazional-socialista di pulizia razziale, al fine di affermare l'imposizione in Germania di una razza ariana incontaminata, sono fatti noti e l'attuazione di questo piano è stato senz'altro facilitato dall'utilizzo delle tecnologie di elaborazione automatizzata dei dati.

Quest'ultima, consentendo la massiccia raccolta di informazioni sulla popolazione, al conseguente fine di suddivisione della stessa in categorie,

---

[12] Per *Scheda Perforata* si intende un supporto di registrazione atto a contenere informazioni utili da utilizzare nelle macchine per il trattamento automatico di dati. Le schede perforate sono fatte di cartoncino e rappresentano l'informazione attraverso la presenza o l'assenza di fori in posizioni predefinite della scheda.

[13] Per *Elaborazione Dati* si intende un qualsiasi procedimento informatico che comporta la conversione dei dati in informazioni dove: con *dato* si intende una raccolta di numeri o lettere che descrivono misure ottenute da un sistema reale; con *informazione* una risposta, dotata di significato, ad una determinata domanda. In altre parole, usando il linguaggio dell'automatica si può definire "elaborazione" quel processo che, a partire da determinati input, produce determinati output dopo una certa manipolazione o trasformazione.

[14] *IBM (International Business Machines)* nacque nel 1884 quando Herman Hollerith fonda la ***Tabulating*** *Machine Company* e brevetta una macchina tabulatrice automatica in grado di leggere schede perforate. La società cambiò nome ufficialmente in IBM nel 1924. È cosa nota il ruolo attivo delle tecnologie inventate dalla società americana nell'ambito delle politiche "razziali" della Germania Nazista. Si cita qui a titolo esemplificativo il saggio di EDWIN BLACK, *L'IBM e l'olocausto. I rapporti fra il Terzo Reich e una grande azienda americana*, Rizzoli, 2001 che descrive in modo dettagliato e documentato il ruolo svolto dall'IBM, attraverso la sua sussidiaria tedesca *Dehomag*, nel censimento della popolazione tedesca del 1933, che portò alla schedatura di milioni di ebrei.

permetteva una facile classificazione in ragione dell'origine razziale, dell'orientamento sessuale, delle opinioni politiche e dello stato di salute.

Volendo fare un esempio pratico di come la tecnica di elaborazione automatizzata dei dati potesse essere d'aiuto agli scopi del regime, basti ricordare la famosa "notte dei cristalli", dove grazie alla possibilità di individuare facilmente i nuclei familiari di origine ebraica, proprietari di attività imprenditoriali, negozi e botteghe sul territorio, furono sferrati attacchi mirati ad intimidire la popolazione ebraica consentendo la totale distruzione delle sole attività appartenenti ad ebrei.

Risulta evidente come in questo contesto storico le innovazioni tecnologiche asservite alle ideologie dei totalitarismi del novecento, si siano configurate come vere e proprie armi di "distruzione di massa" dei diritti umani, in cui i concetti di dignità e libertà furono del tutto annientati.

È proprio dalle macerie di questo periodo buio dell'Europa continentale che nasce, all'alba della fine del secondo conflitto mondiale, la coscienza di implementare la tutela dei diritti fondamentali di libertà e dignità della persona umana anche tramite la gestione di queste nuove tecnologie, aprendo la strada al futuro riconoscimento di un diritto autonomo alla protezione dei dati personali.

Invero, è attraverso l'analisi del profilo inerente il bene giuridico tutelato che si coglie la maggiore differenza tra diritto alla riservatezza e diritto alla protezione dei dati personali.

Se nel diritto alla riservatezza il bene giuridico tutelato è circoscritto alla sfera intima della persona, intesa come quell'insieme di emozioni, pensieri, comportamenti mediante cui si sviluppa la personalità dell'individuo e che si sviluppano all'interno della sacra dimensione privata dello stesso, nel diritto alla protezione dei dati personali assume ruolo centrale il concetto di *dato* o, più in generale, di informazione.

Secondo la definizione prevista all'articolo 4 delle "Disposizioni generali", nel capo primo del nuovo Regolamento Europeo n. 679/2016[15], destinato a disciplinare l'intera materia del diritto alla protezione dati dal 25 maggio 2018, si intende per "dato personale" : «*qualsiasi informazione riguardante una persona fisica identificata o identificabile; si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare 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 della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale*.»

Dunque il bene giuridico tutelato in questo contesto è il complesso di informazioni che permettono di identificare una persona sotto vari aspetti: fisico-somatici, come i tratti del viso o i c.d. "segni particolari", genetici e fisiologici come una particolare patologia o l'individuazione di un segmento di DNA o ancora del gruppo sanguigno di appartenenza ovvero culturali e sociali come, ad esempio, l'adesione ad una particolare comunità, ad una religione o le informazioni contenute in registri pubblici e privati come l'anagrafe.

Tutte queste informazioni sono un patrimonio strettamente personale dell'individuo e anche se rese pubbliche, tramite il consenso dello stesso, devono essere protette da un uso illecito che ne preveda l'acquisizione, la trattazione, la conservazione e la diffusione, direttamente o indirettamente.

Il diritto alla protezione dei dati personali prevede che il soggetto, a cui tali dati si riferiscono, abbia completa disponibilità degli stessi e possa compiere tutti gli atti di disposizione necessari al fine di garantirne l'autenticità, l'aggiornamento e se necessario la cancellazione.

[15] Si ricorda qui che il Regolamento UE 2016/679, insieme alla Direttiva UE 2016/680, rappresentano il c.d. "Pacchetto protezione dati", che riforma l'intera materia il Regolamento per quanto riguarda l'apparato normativo generale, la Direttiva per quanto riguarda il settore della cooperazione giudiziaria e di polizia.

Ci si riferisce, in quest'ultima battuta, al riconoscimento ad opera del recente regolamento europeo del cd. "diritto all'oblio" affermato prima di ora, solo a livello giurisprudenziale.

Quest'ultimo, secondo quanto previsto all'articolo 17 del suddetto Regolamento, prevede il diritto dell'interessato e il corrispettivo obbligo da parte del titolare del trattamento, a procedere senza ritardo ingiustificato alla cancellazione dei dati personali al ricorrere di determinate situazioni, ad esempio qualora i dati non siano più necessari rispetto alle finalità per le quali sono stati raccolti o trattati, qualora vi sia la revoca del consenso, ovvero il trattamento sia illegittimo e infine qualora la cancellazione sia prevista come adempimento ad un obbligo legale previsto dalla normativa UE o di uno Stato membro cui è soggetto il titolare del trattamento.

In conclusione il diritto alla protezione dei dati personali nasce come una tutela protesa a limitare le aspirazioni di controllo globale sugli individui da parte dei poteri forti dello Stato, testimone l'esperienza dei regimi totalitari della prima metà del XX secolo, e si evolve, fino ai giorni nostri, come baluardo a difesa della libertà e della dignità della persona, sempre da forme di controllo indiscriminate sulla popolazione, ma soprattutto, oggigiorno, da un uso distorto delle informazioni che la riguardano sempre più minacciate dall'era digitale e dalle potenzialità, pressoché infinite, delle sue tecnologie.

Tecnologie che, riprendendo le parole del noto giurista Stefano Rodotà, sfidano i vecchi diritti e ne esigono impetuosamente di nuovi[16].

[16] S. RODOTA', *Tecnologie e diritti* , il Mulino, Bologna, 1995, p. 15.

Sezione II

Le Fonti Europee sul Diritto alla Protezione dei Dati Personali

1. Il graduale emergere del diritto alla protezione dei dati personali: le costituzioni europee del secondo dopoguerra

Il diritto alla protezione dei dati personali, come diritto autonomo, a sé stante dal diritto alla riservatezza, non si afferma così rapidamente come ci si sarebbe aspettati a seguito del massiccio uso della tecnica di elaborazione automatizzata dei dati, di cui si è stati testimoni durante i regimi totalitari del novecento.

Invero, le costituzioni degli Stati europei del secondo dopoguerra furono tutte fortemente incentrate sul riconoscimento dei diritti fondamentali dell'uomo, ma non sembrava esserci ancora spazio per il riconoscimento della protezione dati come autentico valore costituzionale.

Tutte le più ispirate costituzioni di quel periodo fanno esplicito riconoscimento dei diritti inviolabili dell'uomo quali la libertà, la dignità e l'uguaglianza.

Si pensi all'articolo 1 della Legge fondamentale della Repubblica di Germania del 23 maggio 1949, rubricato "Protezione della dignità umana" per cui « *La dignità dell'uomo è intangibile. È dovere di ogni potere statale rispettarla e proteggerla. Il popolo tedesco riconosce gli inviolabili e inalienabili diritti dell'uomo come fondamento di ogni comunità umana, della pace e della giustizia nel mondo. I seguenti diritti fondamentali vincolano la legislazione, il potere esecutivo e la giurisdizione come diritti direttamente applicabili*.».

Proprio la Germania, uscita sconfitta dal secondo conflitto mondiale, protagonista, e forse per la prima volta realmente conscia, degli orrori perpetrati dalla dottrina nazionalsocialista contro l'essere umano, e dei quali ne rimane imperitura traccia nella memoria dell'Olocausto, afferma saldamente in apertura del proprio testo costituzionale la "intangibilità" della dignità umana.

Intangibilità intesa, non solo come inviolabilità, ma come "sacralità" della dignità umana.

Quest'ultima non va riconosciuta solamente come valore naturale dell'uomo, come diritto preesistente allo Stato e caratterizzante la forma dello Stato democratico stesso, come essenza stessa dell'essere umano e perciò irrinunciabile, e dunque da rispettare in assoluto, ma l'aspetto della sacra dimensione della dignità umana fa sì che diventi specifico "dovere di ogni potere statale" proteggerla in quanto tale. Ciò in base al principio personalista per il quale al vertice dei valori riconosciuti nell'ordinamento figura la persona nell'intero spettro mediante il quale la sua personalità si sviluppa e per cui lo Stato è al servizio della persona e non viceversa.

A maggior riprova di quanto sopra asserito, la Legge Federale di Germania prosegue riconoscendo come valore di ogni comunità, al fine di mantenere la pace e la giustizia nel mondo, il rispetto dei diritti inviolabili e inalienabili della persona, non limitandosi solo a questo. Esplicitamente riconosce che tali diritti fondamentali costituiscono direttamente limite e insieme vincolo all'esercizio delle funzioni esecutive, legislative e giurisdizionali. Sembra chiara, dunque, la volontà di scongiurare il pericolo che possa ripetersi in futuro uno straripamento dei poteri statali capaci di perpetrare violazioni dei diritti fondamentali dell'uomo in modo continuativo e violento, così come successo durante il Terzo Reich.

Stessa concezione personalista si riscontra anche nella Costituzione della Repubblica Italiana, approvata il 22 dicembre 1947 dall'Assemblea Costituente, ispirandosi anch'essa alla massima estensione della protezione di questi diritti fondamentali a tutela della persona.

Intenzione che venne abilmente realizzata, tramite l'utilizzo di una notevole tecnica giuridica da parte dell'Assemblea, nell'articolo 2 della Costituzione.

La norma costituzionale, nella prima parte, sancisce che «*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità …*».

Riconosce nel senso per cui prende atto del fatto che preesistono all'ordinamento giuridico dei diritti essenziali che fanno indissolubilmente capo alla persona, garantisce nella parte in cui si propone l'obbligo, o forse è meglio dire il dovere, di impegnarsi con tutte le sue articolazioni al fine di salvaguardare, senza operare in alcun modo discriminazioni, l'esercizio e la titolarità dei suddetti diritti. Tutt'al più il loro esercizio può essere limitato soltanto temporaneamente e con il rispetto di precise e determinate garanzie.

Ne consegue che nessuna forma di ingerenza da parte dello Stato, capace di ledere i diritti fondamentali dell'uomo o delle aggregazioni sociali nelle quali esso sviluppa la sua personalità, al di fuori delle modalità di cui sopra, può essere ammessa.

Ancora, si consideri la Costituzione Francese del 4 ottobre 1958 nel cui preambolo sancisce che «*Il Popolo Francese proclama solennemente la sua fedeltà ai diritti dell'uomo …*» oppure la più recente Costituzione Spagnola del 1978 che addirittura dedica ai diritti fondamentali l'intero Titolo I, rubricato per l'appunto "Dei Diritti e Doveri Fondamentali".

In apertura di titolo compare l'articolo 10, che richiama esplicitamente la Dichiarazione Universale dei Diritti dell'Uomo promossa dalle Nazioni Unite e siglata a Parigi nel 1948, nonché i Trattati e Accordi internazionali in materia ratificati dalla Spagna, e che riconosce altresì « *La dignità della persona, i diritti inviolabili che le sono connaturati, il libero sviluppo della personalità, il rispetto della legge e dei diritti altrui sono fondamento dell'ordine politico e della pace sociale.* ».

Risulta evidente, allora, come tutte le democrazie del secondo dopoguerra, tanto quelle più antiche quanto quelle più recenti, abbiano fatto della persona umana, dei suoi valori e della protezione dei suoi diritti fondamentali impegno e dovere improrogabile e indefettibile.

Come detto in apertura di paragrafo, i cataloghi di diritti fondamentali inseriti all'interno dei testi costituzionali non contemplano la protezione dei dati personali, ritagliandole uno spazio autonomo, al fine di limitare ingerenze statali

o anche di privati all'interno del patrimonio informativo di una persona. Forse, non valutando adeguatamente lo sviluppo tecnologico vertiginoso, che in quel tempo, ebbero le tecniche di raccolta ed elaborazione dati, le implicazioni che ebbero per i fini criminali nazisti o che avrebbero potuto esplicare in futuro, i costituenti europei decisero che sarebbe stato sostanzialmente equivalente elaborare una tutela costituzionale, di tali situazioni, attraverso il saldo riconoscimento dei diritti umani quali fondamenta di un ordinamento democratico, dal quale ne deriva come corollario l'impossibilità di qualsiasi ingerenza da parte dei poteri dello Stato e nessuna giustificabile lesione di suddetti diritti. Allo stesso modo adeguato, al fine di tutelare l'indiscriminato controllo tramite la massiccia analisi dei dati riferibili alle persone, ritennero il solo riconoscimento, all'interno del catalogo dei diritti fondamentali, del diritto alla riservatezza, del rispetto della vita privata, familiare e dell'intimità del domicilio.

2. La Convezione Europea dei Diritti dell'Uomo (CEDU): un'occasione mancata per la protezione dei dati personali

La Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali, comunemente abbreviata in CEDU, avrebbe potuto rappresentare un importante trampolino di lancio per l'entrata, nel novero dei diritti fondamentali della persona, del diritto alla protezione dei dati personali.

La Convenzione fu firmata a Roma il 4 novembre 1950 da parte dei dodici stati che all'epoca formavano il Consiglio d'Europa: Belgio, Danimarca, Francia, Grecia, Irlanda, Islanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Regno Unito, Svezia, Turchia.

La CEDU costituiva, e costituisce tuttora, il testo centrale e di riferimento in tema di diritti umani, ciò anche in considerazione del fatto che fosse l'unica, a quei tempi, a essere dotata di un meccanismo giurisdizionale autonomo che

consentisse agli individui di poter esperire reclami al fine di richiedere la tutela dei diritti contenuti nella Convenzione.

A tal proposito, fu istituita nel 1959 la Corte Europea dei Diritti dell'Uomo (anche detta Corte EDU) con sede a Strasburgo, da non confondere con la Corte di Giustizia Europea con sede a Lussemburgo, poiché a differenza di quest'ultima, essendo un'istituzione distinta e autonoma, non appartiene all'Unione Europea.

Malgrado l'ampio utilizzo delle tecniche di elaborazione dei dati personali, durante il periodo dei totalitarismi, tanto le costituzioni dei Paesi europei quanto la Convenzione europea dei diritti dell'uomo non hanno preso in considerazione la possibilità di introdurre una tutela di rango primario all'illecita raccolta, gestione e trattamento delle informazioni riconducibili alla persona.

Le ragioni di tale esclusione sono da ricercare, come affermato da autorevole Dottrina, nel fatto che all'epoca la tecnologia fosse vista principalmente come un mero strumento, come un mezzo asservito ad uno scopo, e non invece come un fattore capace di influenzare le modalità di esercizio di un diritto o addirittura capace di elaborarne di nuovi[17]. A ulteriore supporto dell'idea della tecnologia come mero strumento, rimane il fatto che le neonate costituzioni europee prendono in considerazione, esclusivamente, il rapporto tra stampa e gli altri diritti fondamentali, tralasciando la disciplina e l'analisi di mezzi di informazione che, nel periodo dei totalitarismi in particolare, furono strumenti ben più pregnanti di diffusione di ideologie, propaganda e di controllo del vivere sociale come il cinema e la radio.

Inoltre, determinante fu l'azione delle truppe alleate sul suolo occupato dal regime nazista, subito dopo la fine del secondo conflitto mondiale. Infatti l'esercito americano continuò ad utilizzare i sistemi di archiviazione

[17] F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016, p. 57.

automatizzati di dati in grande quantità, al fine di individuare e perseguire componenti del partito nazista e collaborazionisti sul territorio[18].

Queste e altre ragioni rappresentano la principale motivazione per cui la CEDU, nel suo catalogo di diritti fondamentali, confermi la necessità di una tutela della riservatezza riconoscendo all'articolo 8 il diritto al rispetto della vita privata e familiare, ma non introduca un'apposita norma che riconosca il diritto alla protezione dei dati personali come diritto fondamentale autonomo e differenziato dalla più generale riservatezza.

Non a caso il testo dell'articolo 8 CEDU recita:

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

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

Fondamentali, ai fini della tutela di tale diritto, risultano i confini descritti dal secondo comma dell'articolo in questione. Infatti al secondo comma viene sancito come principio generale l'impossibilità di ingerenza da parte dell'autorità pubblica all'interno della sfera di vita privata e familiare della persona, comprendente inoltre il domicilio e la corrispondenza, capace di violare il diritto alla riservatezza dell'individuo e delle sue comunicazioni interpersonali.

Tale ingerenza, infatti, può essere giustificata soltanto quando sia direttamente prevista dalla legge e necessariamente quando dal bilanciamento, con il diritto di cui parlasi, prevalgano differenti interessi ritenuti, di volta in volta, più meritevoli di tutela: come ad esempio la sicurezza nazionale o economica di un paese, la protezione della collettività sotto gli aspetti della protezione della salute,

[18] *Ibidem.*

della prevenzione di reati o nella più generale protezione dei diritti o libertà altrui.

Interessante è il "parametro" che deve essere ponderato al fine della determinazione, tanto del bilanciamento tra diritti, quanto nella scelta delle modalità con le quali far operare il limite all'esercizio del diritto alla riservatezza, costituito dall'inciso «(*...) una misura che, in una società democratica, è necessaria a (...)*».

I principi di una società democratica sono i valori da tenere in considerazione come parametro di consentita tollerabilità per il quale è accettabile, che il diritto previsto all'articolo 8 CEDU, possa essere temporaneamente limitato. Diventa vero e proprio limite alle intromissioni generalizzate e non motivate da parte dello Stato all'interno della vita della persona e all'inviolabile esercizio dei propri diritti fondamentali, o forse è meglio dire, diventa vero e proprio criterio di legittimità delle ingerenze statali rispetto al diritto al rispetto della vita privata.

3. La nascita, a livello statale, delle prime normative sulla protezione dei dati personali: Germania, Francia e Spagna

Il percorso del diritto alla protezione dei dati personali per affermarsi, sia a livello statale sia a livello europeo, è stato tutt'altro che agevole. Basti pensare che all'alba della Convenzione Europea dei Diritti dell'Uomo ci vollero ben più di venti anni perché comparisse, per la prima volta, una normativa che esplicitamente disciplinasse la protezione dei dati personali in merito alla raccolta massiccia di informazioni in banche dati e al trattamento generalizzato di queste ultime con tecniche automatizzate.

La Germania fu il primo Stato a varare leggi sulla protezione dei dati personali.

Prima legge al mondo in tema fu quella del Land dell'Assia che, già nel 1970, iniziava a predisporre una normativa che tutelasse i lavoratori direttamente da schedature indebite e dalla conservazione, insieme al trattamento, di dati racchiusi in banche dati. Seguirono poi, a livello locale, ulteriori leggi adottate da

altri Lander, a livello federale invece, una legge sulla protezione dei dati personali (*Bundesdatenschutzgesetz o BDSG*).

Il BDSG così come elaborato nel 1977 ebbe vita breve, poiché venne sostituito dalla "Legge per lo sviluppo dell'elaborazione e della protezione dei dati personali" del 1990 a seguito della sentenza del 15 dicembre 1983 del *Bundesverfassungsgericht*[19](Tribunale Costituzionale Federale Tedesco), che costituisce a tal proposito una vera e propria pietra miliare.

Il Tribunale Costituzionale Federale Tedesco, con notevole lungimiranza, intuì per prima le implicazioni e le ripercussioni che un'indiscriminata raccolta e gestione di dati personali potesse rappresentare in termini di lesione dei diritti fondamentali della persona.

Con la sentenza citata, il Tribunale Federale di Germania ha attribuito inequivocabilmente alla tutela dei dati personali un rilievo costituzionale, attraverso l'individuazione di un "diritto all'autodeterminazione informativa", ricostruito come concretizzazione del diritto generale della personalità di cui agli artt. 1 e 2 della Legge Fondamentale Tedesca, che tutelano rispettivamente la dignità umana e i diritti di libertà della persona. Il suo contenuto è individuato nel potere di ciascuno di decidere sostanzialmente, in maniera autonoma e personale, circa la rivelazione e l'utilizzo dei propri dati personali. Dunque il libero sviluppo della personalità presuppone la protezione del singolo dalla memorizzazione, utilizzazione e trasferimento incontrollato di dati personali.

Poco tempo dopo anche la Francia si dotò di una legge in materia: la "*Loi informatique, fichiers et libertés"* n. 17 del 6 gennaio 1978 relativa alla disciplina letteralmente "dell'informatica, dei file e delle libertà" nel settore appunto della conservazione, in banche dati automatizzate pubbliche e private, attraverso l'utilizzo di tecniche informatiche.

Assumono un'importanza cardinale i primi articoli della legge dove: all'articolo 1 è sancito il principio per cui «*L'informatique doit être au service de chaque citoyen… Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de*

[19] BUNDESVERFASSUNGSGERICHT, sentenza n. 209, del 15 dicembre 1983.

l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.» e cioè che l'informatica deve essere al servizio di ogni cittadino e che le tecniche informatiche, comunque utilizzate, non devono attentare né all'identità umana, né ai diritti fondamentali dell'uomo, né alla vita privata, né alle libertà individuali o pubbliche.

Ancora l'articolo 2 stabilisce che nessuna decisione di un tribunale, amministrativa o anche privata, che coinvolga una valutazione della personalità umana, possa essere basata unicamente su di un trattamento automatizzato di dati che descriva il profilo o la personalità dell'individuo coinvolto.

La legge francese n. 17-78 è centrale nel sistema del diritto alla protezione dati, non solo perché per prima crea delle linee-guida all'utilizzo dell'informatica in tema di diritti fondamentali, ma anche perché, sempre per prima, istituisce un'apposita autorità indipendente di controllo sul rispetto di tale legge.

La CNIL (*Commission Nationale de l'Informatique et des Libertes*) difatti si configura come autorità indipendente deputata a garantire il rispetto della legge che la istituisce, ad informare tutti gli interessati in merito ai propri diritti e obblighi tramite audizioni dirette con quest'ultimi, nonché regolare e controllare la conformità delle applicazioni informatiche utilizzate nel trattamento dei dati personali. A tal riguardo la Commissione ha poteri di regolamentazione, controllo e di tipo sanzionatorio.

Nello stesso anno la Spagna, come conseguenza del processo di conversione del regime franchista nell'odierna monarchia parlamentare, la c.d. *"Transición española"*, diede alla luce la *Constitución española de 1978.* Quest'ultima è degna di nota perché fu in assoluto la prima tra le costituzioni democratiche moderne ad inserire e tutelare direttamente a livello costituzionale, come autonomo diritto fondamentale della persona, il diritto alla protezione dei dati personali. Dunque l'articolo 18 della Costituzione spagnola accoglie e cristallizza, su di un piano tutto nuovo, quell'orientamento che dai primi anni settanta iniziava a farsi strada tra le giurisprudenze europee più accorte e che iniziavano a intuire una stretta correlazione tra sviluppo della tecnologia ed

evoluzione di nuovi diritti nonché della protezione di quelli più antichi. Infatti l'articolo di cui parlasi prevede al primo comma che: «*Si garantisce il diritto alla tutela dell'onore, dell'intimità personale e familiare e della propria immagine.*» e poi, al quarto comma che: «*La legge limiterà l'uso dell'informatica per tutelare l'onore, l'intimità, personale e familiare dei cittadini e il pieno esercizio dei loro diritti.*». Le previsioni "programmatiche" contenute nell'articolo 18 della Costituzione spagnola sono state attuate con l'adozione di leggi apposite: come quella del 1982 sull'onore, quella del 1984 sulle intercettazioni telefoniche, ripresa nel 1992 dalla cd. "*Legge Corcuera*" sulla sicurezza urbana. Per molto tempo l'unica parte dell'articolo 18 che non è stata presa in considerazione fu proprio la disposizione del quarto comma, fino a quando nel 1992 entrò in vigore la "*Ley Organica de regulacion del tratamiento automatizado de los datos de caracter personal*". La Legge organica[20] del 1992 è stata sostituita successivamente dalla legge n. 15 del 1999 (sempre organica), con la quale è stata data attuazione anche in Spagna alla Direttiva europea 95/46/CE.

Orbene data l'evoluzione normativa in tema di privacy generalmente intesa, e protezione dati in senso più specifico, tra l'inizio degli anni settanta e i primi anni novanta, risultava comunque un quadro d'insieme molto diversificato e a tratti incompatibile tra un paese e l'altro, capace di comportare seri problemi di interpretazione e applicazione nei casi in cui due Stati si fossero trovati a dover trattare, raccogliere o scambiare dati tra loro.

Al fine di risolvere tale *impasse* era necessaria una regolamentazione comune che racchiudesse i principi in tema di protezione dei dati personali condivisi dalla maggioranza dei Paesi europei e che fosse, allo stesso tempo, un'occasione a livello Comunitario di una congiunta evoluzione. Tali obiettivi vennero perseguiti, nell'ambito dell'ordinamento CEDU, dalla Convenzione n. 108 del 28 gennaio 1981 adottata dal Consiglio d'Europa e invece, a livello dell'Unione Europea, dalla Direttiva Europea 95/46/CE nonché dall'opera di costruzione

[20] Per legge organica si intende una legge di rango superiore rispetto a quella ordinaria, paragonabile alle nostre leggi costituzionali.

della Carta dei diritti fondamentali dell'Unione Europea (Carta di Nizza 2000), e dall'opera integrativa del Trattato di Lisbona al fine di creare un corpo normativo unitario riguardante la protezione dei dati personali.

4. La Convenzione CEDU 108/1981/CE: l'inizio di un nuovo percorso

Lo scenario giurisprudenziale europeo fin qui descritto si presenta come un "pentolone di riforma" in continua ebollizione dal quale fuoriescono bolle di vapore cariche di innovazione e ispirate da valori di garanzia. Nonostante ciò, il quadro giuridico generale si presentava ancora molto frammentato e di difficile compatibilità non solo pratica, ma anche ermeneutica, data specialmente dalle sottili differenze riscontrabili tra un paese all'altro, che a seconda del percorso storico affrontato nella elaborazione di un concetto di privacy facevano leva, a volte su di un costrutto culturale strettamente legato alla riservatezza, come diritto alla difesa della libertà della vita personale e familiare, altre volte invece, ad un concetto fondato sulla protezione dei dati personali come libertà dal controllo statale attuata tramite la raccolta in banche dati automatizzate.

Di conseguenza l'importanza della Convenzione di Strasburgo n. 108 del 28 gennaio 1981 "sulla protezione delle persone rispetto al trattamento automatizzato dei dati di carattere personale", si coglie con evidenza dal solo scopo di cui essa si fa portatrice nell'articolo primo: «*(...) garantire, sul territorio di ogni Parte, ad ogni persona fisica, qualunque siano 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.*», e nel preambolo ove è sancito il principio secondo cui la libera circolazione delle informazioni tra i popoli non può prescindere assolutamente dalla tutela dei diritti e delle libertà fondamentali di ciascuno.

Per la prima volta, sul suolo europeo e per mezzo della proposta del Consiglio d'Europa, riesce l'impresa di creare un sistema unitario, ideato e realizzato per

facilitare l'azione dei diversi paesi all'interno delle diversificate trame del panorama europeo dell'epoca (come ad esempio quelle dell'emergente Mercato Unico). Tutto ciò avvenne tramite la predisposizione di una disciplina generale che dettava i principi generali da rispettare ed attuare in tema di protezione dati.

Inoltre, ulteriore particolarità del sistema risiede nel fatto che, non solo la Convenzione, in quanto proposta dal Consiglio d'Europa, ha il carattere e l'obbligatorietà di un accordo internazionale, ma anche che essa è aperta, in considerazione del fatto che, diversamente dalle altre convenzioni CdE, permette la ratifica a qualunque altro Stato, anche non facente parte del Consiglio d'Europa stesso, previo invito da parte del Consiglio dei Ministri.

La Convenzione senza troppe pretese di specificazione, ma pur sempre con occhio vigile, nei primi due capitoli, quelli inerenti le disposizioni generali e i principi in materia, cerca di enucleare un "*principles common core"*, un denominatore comune minimo di principi e garanzie a cui gli Stati devono rifarsi: minimali, ma tutti irrinunciabili.

In modo specifico la Convenzione n. 108/1981 si incentra sulla tutela delle sole persone fisiche, con riguardo alle possibili violazioni dei diritti umani fondamentali tramite l'elaborazione automatizzata dei dati di carattere personale che le riguardano. Da ciò ricaviamo direttamente che rimangono al di fuori della copertura predisposta dalla disciplina convenzionale tanto le persone giuridiche, quanto i sistemi di elaborazione non automatizzati di dati, anche quando connessi con sistemi automatizzati.

A parte questa considerazione, dal testo della Convenzione si possono cogliere importanti principi in tema di protezione dati, che risulteranno fondamentali ai fini dell'evoluzione del diritto stesso e che saranno adottati anche dai successivi atti principali (per es. gli atti dell'Unione Europea) in materia.

Innanzitutto la Convenzione all'articolo 2 dà le definizioni di "dato di carattere personale" ed "elaborazione automatizzata": definendo il primo come «*ogni informazione relativa ad una persona fisica identificata o identificabile (persona interessata)*» e la seconda come un'attività che «*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».

Ulteriori disposizioni importanti in merito ai dati vengono prese in considerazione negli articoli successivi.

All'articolo 5 intitolato "Qualità dei Dati" sono descritte le caratteristiche e le modalità affinché i dati personali possano ritenersi di qualità adeguata, essi devono essere:

a) Ottenuti ed elaborati in modo lecito e corretto;
b) Registrati per scopi determinati e legittimi ed impiegati in una maniera non incompatibile con detti fini;
c) Adeguati, pertinenti e non eccessivi riguardo ai fini per i quali vengono registrati;
d) Esatti e, se necessario, aggiornati;
e) Conservati in una forma che consenta l'identificazione delle persone interessate per una durata non superiore a quella necessaria ai fini per i quali sono registrati.

Altro principio fondamentale è quello previsto all'articolo 6 dove viene introdotta una speciale categoria di dati c.d."sensibili", allo scopo di offrire un'adeguata risposta ai crescenti timori di un'opinione pubblica sempre più accorta rispetto a indiscriminate schedature degli aspetti più intimi delle persone o di atteggiamenti discriminatori fondati su tali dati.

Infatti, i dati sensibili sono composti da quella tipologia di informazioni caratterizzanti una persona e capaci di rilevare l'origine razziale, le opinioni politiche, le convinzioni religiose, lo stato di salute e l'orientamento sessuale nonché quelle relative a condanne penali di un individuo. Tali dati, è prescritto dall'articolo 6, non possono essere elaborati con tecniche automatizzate a meno che non vengano previste garanzie adatte. Bisogna specificare che l'elaborazione e la circolazione di questa tipologia di dati non è generalmente vietata soltanto sulla base della "intimità" dell'informazione, ma specialmente perché, più di

altre tipologie di dati, questi, possono essere fonte di discriminazione e in quanto tale, ostacolo all'evolversi della personalità di un individuo specialmente all'interno della società.

Procedendo all'analisi del testo convenzionale, gli articoli 7 e 8 disciplinano rispettivamente la sicurezza dei dati e le garanzie per la persona interessata.

Il primo prevede che debbano porsi in essere "adeguate misure di sicurezza" nei casellari automatizzati contro la distruzione e la perdita accidentale o non autorizzata, ovvero contro gli accessi, la modifica e la diffusione non autorizzata.

Il secondo, invece, prevede che alla persona interessata debbano essere riconosciute determinate facoltà inerenti la conoscenza e la gestione dei suoi dati tra cui: conoscere l'esistenza di un casellario automatizzato contenente dati a carattere personale nei suoi riguardi nonché i fini principali per cui sono conservati, ovvero l'identità e la residenza/sede amministrativa del responsabile del casellario; avere la possibilità di ottenere la rettifica o la cancellazione di tali dati se elaborati in violazione dei principi di cui agli articoli 5 e 6; avere la possibilità di un esperire un ricorso qualora non venga dato tempestivo seguito ad una richiesta di prendere visione, rettificare o cancellare tali dati.

I principi finora descritti sono previsti come generalmente applicabili, ma non per questo considerati come assoluti. Infatti sono previste all'articolo 9 condizioni tassative per le quali uno Stato può derogare ai principi espressi negli articoli che lo precedono. Sempre prevedendo come parametri di legittimità dell'azione statale e di tutela dei diritti fondamentali, la "democraticità" e la "necessità" della misura, la deroga può operare qualora risultino in pericolo beni quali:

a) la protezione della sicurezza dello Stato, la sicurezza pubblica, gli interessi monetari dello Stato o la repressione dei reati;
b) la protezione della persona interessata e dei diritti e delle libertà altrui.

Di notevole interesse, infine, specialmente in chiave di analisi della successiva Direttiva Europea 95/46, poiché rappresenta un carattere di distinzione con quest'ultima, è l'articolo 12 della Convenzione CEDU n. 108/1981.

L’articolo 12 è rubricato “Movimento oltre frontiera di dati a carattere personale e diritto interno” e in maniera più che esplicita al secondo paragrafo enuncia come principio generale quello della trasferibilità oltre frontiera dei dati trattati in modo automatizzato o raccolti per essere poi elaborati in tal senso.
Al contrario della direttiva 95/46, che stabilirà in linea generale il divieto di trasferimento dei dati trattati in modo automatizzato, la Convenzione prevede che le Parti non possano proibire il trasferimento oltrefrontiera di tali dati e tanto meno sottoporre il trasferimento a particolari autorizzazioni.
Tuttavia al paragrafo terzo sono previste due possibilità di deroga a tale principio di trasferibilità e cioè quando:

a) la legislazione dello Stato “trasferente” prevede una regolamentazione specifica per alcune categorie di dati a carattere personale o in merito ai casellari automatizzati in cui essi sono custoditi, in ragione della natura di detti dati o casellari, a meno che la regolamentazione dell'altra Parte offra una protezione equivalente;
b) il trasferimento sia effettuato verso il territorio di uno Stato non contraente per il tramite di un’altra Parte, al fine di evitare che simili trasferimenti si traducano in un aggiramento della legislazione della Parte dal cui territorio parte il flusso di dati o delle garanzie previste dalla Convenzione.

La Convenzione di Strasburgo è stata e continua ad essere un testo di grande importanza giuridica in materia di protezione dei dati personali.
Non solo essa rappresenta l’autentico tassello finale del lungo percorso che ha portato alla definitiva comprensione e al riconoscimento del diritto alla protezione dei dati personali come vero e proprio diritto fondamentale a tutela della libertà degli individui, definitivamente separato oramai dal concetto “madre” di riservatezza, ma indubbiamente rappresenta un innegabile punto di svolta poiché, ponendosi come normativa sovranazionale, cambia “le regole del gioco” sancendo una volta per tutte principi che non potranno più essere disattesi

dalle legislazioni statali e indicando il primo passo sulla strada da seguire per il futuro legiferare della protezione dei dati personali.

5. I primi passi verso la creazione di una normativa dell'Unione Europea in tema di protezione dei dati personali: ragioni alla base dell'esigenza di un cambiamento

Rispetto all'esperienza degli Stati europei, all'azione del "Sistema" nato dalla Convenzione EDU e dell'attività in tema di diritti umani del Consiglio d'Europa, e della protezione dati nello specifico, l'Unione Europea è stata l'ultima organizzazione internazionale nel tempo a dotarsi di una normativa a riguardo. Ciò si può spiegare anzitutto in una sostanziale differenza di competenze o di missione. Inizialmente le competenze comunitarie erano orientate essenzialmente verso il campo d'interesse economico, mentre il Consiglio d'Europa è stato istituito per promuovere e diffondere in Europa la democrazia ed il rispetto dei diritti fondamentali.

Nel tempo, alla progressiva espansione dello spazio comunitario che si è sviluppato fino a contare 28 Stati membri e coprire un'area europea importante e molto più omogenea rispetto a quella del Consiglio d'Europa, ha fatto seguito una graduale integrazione tra gli Stati membri che è andata ben oltre le iniziali competenze relative al mercato comune. Ma, mentre tutti gli Stati dell'Unione facevano parte del Consiglio d'Europa, l'Unione come tale non partecipava al sistema della Convenzione europea dei diritti dell'uomo, dichiaratasi incompetente a ratificarne l'adesione. Rimanevano così, di competenza esclusiva della Corte EDU, l'interpretazione e applicazione dei diritti fondamentali della Convenzione.

Nonostante ciò i diritti umani, pur non essendo a quel tempo per l'Unione la ragion d'essere, a differenza della missione "naturale" del Consiglio d'Europa e della CEDU, entrarono inevitabilmente a far parte del diritto enunciato e del

diritto vivente dell'Unione, anche e soprattutto nell'applicazione pratica[21]. Applicazione pratica che poteva risultare più che problematica data la duplicazione della tutela giudiziaria in tema di diritti umani che si andava profilando.

La costruzione del Mercato Unico, come obiettivo prefissato dai Trattati di Roma del 1957, esigeva, oltre alla caduta delle frontiere doganali, la piena attuazione delle quattro libertà simbolo dell'integrazione comunitaria: la libera circolazione delle merci, delle persone, dei capitali e la libera prestazione di servizi.

Il Mercato Unico così come ideato, insieme al definitivo abbattimento delle barriere doganali avvenuto ad opera del Trattato di Maastricht nel 1993 (istitutivo dell'Unione Europea, benché ancora suddivisa nella struttura a tre pilastri), imponevano, senza ritardi, di superare le frontiere immateriali costituite dalle diverse leggi nazionali in materia di protezione dei dati personali[22].

A tal fine si rendeva necessaria una normativa adeguata e aggiornata in tema di dati personali (e di diritti fondamentali in generale), ma soprattutto che fosse di origine comunitaria, in modo tale da rendere efficiente il funzionamento del Mercato Unico e, allo stesso tempo di ridisegnare la competenza per tutte quelle controversie inerenti diritti umani fondamentali (non più solo Corte EDU, ma anche Corte di Giustizia Europea), violati però all'interno delle fitte trame del sistema Unione Europea. Tutto ciò fu realizzato per mezzo dell'adozione di due importanti atti da parte dell'Unione Europea: prima con la direttiva 95/46/CE, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati; dopo con l'emanazione della Carta dei diritti fondamentali dell'Unione europea proclamata a Nizza (2000 e 2007) e inclusa nel Trattato di Lisbona entrato in vigore nel 2009.

[21] V. ZAGREBELSKY, *La prevista adesione dell'Unione Europea alla Convenzione europea dei diritti dell'uomo*, in www.europeanrights.eu/public/commenti/Adesione_Zagrebelsky.doc, 2007.

[22] F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016, p. 65.

5.1. L’arrivo sulla scena della Direttiva Europea 95/46/CE

La Direttiva europea 95/46/CE ha costituito per molto tempo il testo di riferimento, a livello europeo, in tema di protezione dei dati personali e, non a caso, è stata denominata “Direttiva Madre”.

Bisogna dire fin da subito che la Direttiva fa riferimento tanto all’articolo 8 CEDU, quanto alla Convenzione n.108/198, ma senza dubbio ne specifica e amplifica contenuto e portata, a volte capovolgendo orientamenti affermati dalle precedenti legislazioni sul tema.

All’epoca, l’Unione Europea risultava ancora suddivisa nella tradizionale struttura a tre pilastri di cui: il primo pilastro riguardava le Comunità Europee (CEE), il mercato comune europeo, l'unione economica e monetaria; il secondo affrontava la Politica Estera e di Sicurezza Comune (PESC), ossia la costruzione di una politica unica verso l'esterno; il terzo, la Cooperazione giudiziaria e di polizia in materia penale (GAI), era rivolto alla costruzione di uno spazio europeo di libertà, sicurezza e giustizia, in cui vi fosse collaborazione contro la criminalità a livello sovranazionale.

Orbene, la disciplina della direttiva del ’95 è nata nell’ambito della Comunità europea e perciò destinata ad operare nell’ambito del primo pilastro.

Per la prima volta, sul suolo europeo, al fine di rendere più efficaci le quattro libertà, il mercato unico e lo sviluppo libero della personalità dell’individuo, l’UE rispondeva con una normativa comune tale da garantire una protezione specifica ai dati delle persone che, dall’abbattimento delle frontiere, erano sì più liberi nella circolazione, ma allo stesso tempo più vulnerabili da attacchi “senza confini”.

Forse da parte del legislatore europeo ci si sarebbe aspettati una diversa forma dell’atto con il quale attuare la disciplina comune sulla protezione dei dati personali, più verosimilmente un regolamento (di fatto lo strumento scelto per la nuova disciplina recentemente approvata nel 2016). Date le caratteristiche del regolamento quali la portata generale, l’obbligatorietà in tutti i suoi elementi e la

diretta applicabilità, sarebbe stato senz'altro il mezzo più idoneo al fine di evitare controversie, lacune esegetiche o diverse interpretazioni tra un Paese e l'altro.
Il legislatore europeo però ha optato per l'adozione di una direttiva d'armonizzazione con lo scopo di stabilire i principi generali e fondanti la materia e una serie di regole, non aventi carattere immediatamente vincolante, ma che avrebbero obbligato gli Stati Membri ad adeguarvi le proprie legislazioni nazionali entro il termine predisposto dalla direttiva stessa.
In ogni caso la Direttiva si è dimostrata nel tempo uno strumento agile e utile favorendo, da un lato, un processo di omogeneizzazione dei livelli di tutela dei diritti, indipendentemente dall'ordinamento statale di riferimento, dall'altro, arricchendo i contenuti dei diritti riconosciuti dalle singole Costituzioni.
La Direttiva 95/46/CE tutela le persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati e si applica tanto ai dati trattati con mezzi automatici, ad esempio banche dati informatiche, quanto ai dati contenuti o destinati a figurare in archivi non automatizzati, come gli archivi tradizionali in formato cartaceo. Quest'ultima parte rappresenta già una differenza sostanziale con la Convenzione CEDU del 1981, la cui disciplina era indirizzata esclusivamente al trattamento di dati presso archivi automatizzati, mentre il campo d'applicazione della Direttiva del '95 descritto all'articolo 3, sembra andare oltre ricomprendendo: il «*trattamento di dati personali interamente o parzialmente automatizzato nonché il trattamento non automatizzato di dati personali contenuti o destinati a figurare negli archivi*».
Inoltre, la Direttiva specifica al paragrafo 2 che le disposizioni non si applicheranno a quei trattamenti di dati personali che sono effettuati in ambito di attività che non competono al diritto comunitario (aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e le attività dello Stato in materia di diritto penale), nonché a quei trattamenti effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.
Ulteriori tratti distintivi e di innovazione si riscontrano sicuramente nelle definizioni inserite all'articolo 2, che specificano e ampliano le nozioni già

esistenti nella Convenzione e inseriscono nuove figure all'interno del panorama della protezione dati. Quando la Direttiva dà la definizione di "dato personale" non si limita solamente a definirlo come qualsiasi informazione che rimanda ad una persona identificata o identificabile, ma specifica che si considera "identificabile": «*la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento ad un numero di identificazione o ad uno o più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale*».

La Direttiva specifica inoltre, rispetto alla descrizione di elaborazione automatizzata adottata dalla Convenzione n. 108/1981, in cosa consista il trattamento di dati personali aggiungendo ulteriori azioni alle quali possono essere sottoposti i dati di carattere personale come: «*la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione o la modifica, l'estrazione, la consultazione, l'impiego, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, nonché il congelamento, la cancellazione o la distruzione*», compiute con o senza l'ausilio di processi automatizzati. Risulta evidente come questa nuova definizione più ampia e se vogliamo tecnica, sia molto più capace di abbracciare operazioni tecnologiche più avanzate rispetto alla semplice raccolta e "schedatura" dei dati e come sia capace altresì di adattarsi a una futura evoluzione delle tecniche informatiche e delle comunicazioni.

Seguono le definizioni rispettivamente di responsabile e di incaricato del trattamento.

Per responsabile del trattamento si intende la persona fisica, giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che determina le finalità e gli strumenti del trattamento di dati personali, mentre per incaricato del trattamento ci si riferisce sempre alla stessa gamma di soggetti, ma che hanno il compito di elaborare i dati per conto del responsabile del trattamento.

Per quanto riguarda i principi in tema di qualità dei dati e del trattamento la Direttiva Madre non si discosta di molto dalla Convenzione n.108, anche se è ben visibile un'operazione di specificazione e di ampliamento non poco rilevante.

I dati personali devono pur sempre essere ottenuti, trattati lealmente e lecitamente, nonché raccolti per finalità determinate, esplicite e legittime, ed il successivo trattamento non deve essere incompatibile con tali finalità.

Inoltre i dati devono risultare adeguati e pertinenti in modo tale da rispettare le finalità per le quali vengono raccolti e trattati; esatti e, quando necessario, devono essere aggiornati.

Vengono riprese le misure di sicurezza, previste ex articolo 7 della Convenzione n.108/1981, che prevedono l'obbligo da parte del responsabile di porre in essere tutte le misure ragionevoli per cancellare o rettificare i dati inesatti o incompleti rispetto alle finalità per le quali sono rilevati o sono successivamente trattati, cancellati o rettificati.

Infine i dati devono essere conservati, in modo da consentire l'identificazione delle persone interessate, per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per le quali sono rilevati o sono successivamente trattati.

Ancora la Direttiva, in modo innovativo, decide di circoscrivere ad una serie di condizioni determinate la possibilità di effettuazione del trattamento dei dati personali, prevedendo che quest'ultimo possa essere disposto quando: sia fonte di un determinato obbligo avente origine contrattuale privata, e quando risulti fondato direttamente in una disposizione di legge, quale obbligo facente capo al responsabile del trattamento, oppure quando si riscontri la necessità di salvaguardare ulteriori beni "superiori" come l'interesse vitale della persona interessata, l'esecuzione di un interesse pubblico o ancora, sia necessario al perseguimento di un interesse legittimo del responsabile del trattamento, a condizione però, che non prevalgano l'interesse, i diritti e le libertà fondamentali della persona interessata.

Cito per ultima, ma non per importanza, la condizione di cui alla lettera a) dell'articolo 7 della Direttiva, la quale innegabilmente segna una delle principali novità in tema di diritto alla protezione dei dati personali.

Alla lettera a) il legislatore europeo afferma che condizione essenziale, affinché possa essere predisposto il trattamento dei dati personali di taluno, è che *«la persona interessata (abbia) manifestato il proprio consenso in maniera "inequivocabile"*» . In questo modo l'istituto del consenso assume un ruolo centrale e determinante all'interno della protezione dati, arrivando ad identificare addirittura il primo e fondamentale criterio di legittimità del trattamento. Le caratteristiche del consenso vengono inoltre descritte sempre all'articolo 2 "Definizioni" per il quale il consenso deve essere: *«(*una*) qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento.* »

Dunque in linea generale nessun trattamento è lecito se non sia stato prestato un consenso libero, cioè privo di alcun tipo di costrizione fisica o morale, specifico, cioè rivolto verso quel determinato e individuato processo di trattamento dei propri dati personali, e informato in modo tale che la persona interessata sia consapevole dei fini e delle modalità di quel trattamento.

Ciò nonostante anche questo principio soffre delle eccezioni per le quali il consenso non si reputa né presunto, né necessario quando il trattamento debba essere effettuato per motivi inerenti il pubblico interesse o nell'interesse legittimo del responsabile del trattamento o dei terzi che ricevono i dati.

A parte questo, a dimostrazione della centralità che assume ora nella protezione dei dati personali, il consenso offre una tutela rafforzata quando si parla dei c.d. dati sensibili. Infatti l'articolo 8 come principio generale afferma l'impossibilità di trattare quei dati personali capaci di rivelare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale. Merita un'attenzione particolare e una tutela rafforzata tale categoria di dati in quanto,

come abbiamo detto in precedenza, la divulgazione di informazioni di questo genere possono rappresentare un veicolo diretto per la discriminazione di una persona in vari ambiti della propria vita: sociale, professionale e anche familiare.
Tuttavia anche questo principio non è assoluto. Esso cede alle condizioni previste dal paragrafo 2 dell'articolo 8, tutte condizioni va detto, estremamente garantiste tra le quali figura appunto il consenso "rafforzato", poiché la persona interessata al fine di permettere il trattamento dei propri dati sensibili, deve prestare un consenso "esplicito", non più solamente inequivocabile.
Ulteriore nota di distinzione tra Direttiva e Convenzione risulta dalla disciplina in tema di trasferimento di dati verso Paesi terzi prevista all'articolo 25 della Direttiva 95/46. Il legislatore europeo qui, rispetto l'articolo 12 della Convenzione, attua un vero e proprio cambiamento di impostazione: se nella precedente normativa CEDU era imposto agli Stati il divieto di negare il trasferimento o condizionarlo a specifiche autorizzazioni, salvo determinate ipotesi, ora la Direttiva stabilisce che in linea di principio il trasferimento non può aver luogo a meno che il Paese terzo di cui trattasi garantisca un livello di protezione adeguato. L'adeguatezza della tutela predisposta dal Paese destinatario dei dati diventa condizione necessaria affinché il trasferimento dei dati possa avvenire. Il criterio dell'adeguatezza è soggetto ad attenta verifica da parte della Commissione UE, che su richiesta di uno Stato Membro, e secondo la procedura di cui all'articolo 31 comma 2 della Direttiva (parere del Comitato), constata se un Paese terzo abbia i requisiti di tutela adeguati secondo la sua legislazione nazionale o gli impegni internazionali presi o altrimenti avvia le negoziazioni per porre rimedio o pone in essere le misure necessarie a vietare il trasferimento.
L'effetto maggiore derivante dalla disciplina del trasferimento dei dati, nell'ambito comunitario, è senz'altro quello di affermare il principio del mutuo riconoscimento tra Stati Membri tramite l'adozione del criterio dello stabilimento.

Il criterio dello stabilimento (articolo 4 "*Diritto Nazionale Applicabile*") fa sì che venga applicata la normativa di protezione dati dello Stato in cui ha sede lo stabilimento principale del titolare del trattamento. Questo fu il principale veicolo di riforma mediante il quale si arrivò al definitivo superamento di quelle frontiere astratte, limitanti la circolazione dei dati personali sul suolo europeo.

Infine ulteriore innovazione apportata dalla nuova normativa comunitaria fu l'istituzione delle Autorità di Controllo[23] e del c.d. Gruppo Articolo 29[24].

È previsto all'articolo 28 l'obbligo da parte di ogni Stato Membro di istituire sul proprio territorio almeno una Autorità di controllo incaricata di sorvegliare sulla corretta applicazione della Direttiva come adottata dallo Stato. È previsto inoltre che le suddette autorità debbano essere consultate al momento dell'elaborazione delle misure regolamentari o amministrative in tema di trattamento di dati personali.

Tali autorità sono pienamente indipendenti nell'esercizio delle funzioni loro attribuite e ogni autorità di controllo dispone in particolare:

---

[23] Per *Autorità Amministrative Indipendenti* (c.d. autorità garanti o di controllo) si intendono generalmente, quei soggetti o enti pubblici, istituiti con legge, che esercitano in prevalenza funzioni amministrative in ambiti considerati sensibili o di alto contenuto tecnico (concorrenza, *privacy*, comunicazioni ecc.), tali da esigere una peculiare posizione di autonomia e di indipendenza nei confronti del Governo, allo scopo di garantire una maggiore imparzialità (cd. neutralità) rispetto agli interessi coinvolti. Nello specifico il Garante per la Privacy interviene in tutti i settori, pubblici e privati, nei quali occorre assicurare il corretto trattamento dei dati e il rispetto dei diritti fondamentali delle persone: in particolare, banche e assicurazioni, giornalismo, giustizia e polizia, internet, imprese, lavoro, marketing, nuove tecnologie, ordini professionali, partiti, pubblica amministrazione, sanità, società, scuola, telecomunicazioni.
Si veda per una sintetica descrizione delle competenze dell'Autorità garante per la protezione dei dati personali CENTRO DI RICERCA E TUTELA DEI CONSUMATORI E DEGLI UTENTI, *Guida pratica agli organismi di regolazione e controllo a tutela dei consumatori*, su www.centroconsumatori.tn.it, pdf, p.5; si veda anche ENCICLOPEDIA TRECCANI ONLINE, www.treccani.it, definizione *Autorità amministrative indipendenti.*

[24] Il *Gruppo di lavoro articolo 29* (*Working Party article 29 o WP29*) è il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati istituito dall'articolo 29 della direttiva europea 95/46. Questa prevede vari compiti da affidare ai membri dei Garanti nazionali, che quindi si riuniscono a tale scopo. Il Gruppo è un organismo consultivo indipendente, composto da un rappresentante della autorità nazionali, dal Garante europeo della protezione dei dati(GEPD) e da un rappresentante della Commissione. Il presidente è eletto dal Gruppo al suo interno ed ha un mandato di due anni, rinnovabile una sola volta. Il Gruppo adotta le sue decisioni a maggioranza semplice dei rappresentanti delle autorità di controllo. Il suo compito principale è assicurare che le autorità di controllo nazionali seguano interpretazioni comuni della normativa europea in materia. Il Gruppo ha sempre prestato particolare attenzione alle tematiche della rete Internet nell'ambito della protezione dei dati, e questo anche per colmare le lacune della direttiva 95/46, nata in un periodo in cui il fenomeno "internet" non era ancora esploso in tutte le sue potenzialità. GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Gruppo di lavoro ex Articolo 29*, su www.garanteprivacy.it.

a) di poteri investigativi, come il diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo;
b) di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti, quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali;
c) del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della direttiva ovvero di adire per dette violazioni le autorità giudiziarie.

Inoltre qualunque persona può, in particolare, chiedere direttamente a un'autorità di controllo di verificare la liceità di un trattamento e quest'ultima la informa dell'avvenuta verifica e degli eventuali riscontri.

In maniera ancora più innovativa viene previsto che le autorità di controllo collaborino tra loro nella misura necessaria allo svolgimento dei propri compiti, in particolare scambiandosi ogni informazione utile, al fine di rendere efficiente l'implementazione della disciplina e di diffondere il più possibile un'interpretazione di diritto conforme e comune su tutto il territorio.

Invece, il Gruppo per la tutela della persone con riguardo al trattamento dei dati personali, denominato anche il "Gruppo articolo 29" (in inglese *Working Party 29* - WP29), è un organismo a carattere consultivo anche esso indipendente.

La composizione del Gruppo è varia, in modo tale da far confluire vari interessi senza compromettere l'indipendenza e la democraticità del sistema.

Infatti il Gruppo è composto da un rappresentante delle autorità di controllo di ciascuno Stato membro, da un rappresentante delle autorità per le istituzioni e gli organismi comunitari, nonché da un rappresentante della Commissione.

Tra i compiti più importanti del Gruppo rientrano:

a) l’esame di ogni questione relativa l'applicazione delle norme nazionali di attuazione della presente Direttiva per contribuire alla loro applicazione omogenea;
b) la formulazione di un parere sul livello di tutela nella Comunità e nei paesi terzi, a supporto del lavoro della Commissione;
c) consigliare la Commissione in merito a ogni progetto di modifica della presente Direttiva ai fini della tutela dei diritti e delle libertà delle persone fisiche con riguardo al trattamento di dati personali.

Il Gruppo inoltre ha il compito di informare prontamente la Commissione, qualora constati che tra le legislazioni o la prassi degli Stati membri si verifichino divergenze tali da pregiudicare l'equivalenza della tutela nella Comunità e può formulare, direttamente di propria iniziativa, raccomandazioni su qualsiasi questione riguardante la tutela delle persone fisiche.

Infine il Gruppo ha l’obbligo di redigere una relazione annuale sullo stato della tutela delle persone fisiche in merito al trattamento dei dati personali nella Comunità e nei paesi terzi e di trasmetterla alla Commissione, al Parlamento europeo e al Consiglio. La relazione dopo essere stata visionata sarà oggetto di pubblicazione.

5.2. Un nuovo passo in avanti per il Diritto alla Protezione dei Dati Personali: la Carta di Nizza

La Carta dei Diritti Fondamentali dell’Unione Europea, proclamata a Nizza nel 2000, rappresentò ancora un piccolo passo in avanti per il diritto alla protezione dei dati personali. La volontà era quella di creare una Costituzione dell’Unione Europea, intenzione che però incontrò varie opposizioni per le quali solo nel 2007, grazie al Trattato di Lisbona, riuscì ad ottenere piena efficacia.

La Carta nasceva per dare risposta ad una sempre maggiore richiesta di certezza del diritto nell’ambito delle complesse dinamiche economiche, commerciali e

giurisdizionali che l'Unione Europea si ritrovava a dover affrontare, specialmente in tema di diritti umani.

Sempre più incombente, si presentava la necessità di redigere un documento nel quale confluissero per iscritto i principi in tema di diritti umani e delle tradizioni costituzionali comuni agli Stati Membri.

Le soluzioni che si prospettavano erano sostanzialmente di due tipi: da un lato, vi era la possibilità per la Comunità europea di accedere alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU), uno strumento regionale già in vigore, teso a proteggere i diritti umani e sotto la supervisione della Corte europea dei diritti dell'uomo. Tale opzione, tuttavia, fu accantonata dopo che la Corte di giustizia europea, nel suo famoso parere n. 2/94, affermò che: «*Allo stato attuale del diritto comunitario, la Comunità non ha la competenza per aderire alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, in quanto, da un lato, nessuna disposizione del Trattato attribuisce alle istituzioni comunitarie, in termini generali, il potere di dettare norme in materia di diritti dell'uomo o di concludere convenzioni internazionali in tale settore (...) l'adesione della Comunità alla Convenzione europea dei diritti dell'uomo determinerebbe una modificazione sostanziale dell'attuale regime comunitario di tutela dei diritti dell'uomo, in quanto comporterebbe l'inserimento della Comunità in un sistema istituzionale internazionale distinto (...) Una tale modifica del regime della tutela dei diritti dell'uomo nella Comunità, le cui implicazioni istituzionali risulterebbero parimenti fondamentali sia per la Comunità sia per gli Stati membri, rivestirebbe rilevanza costituzionale ed esulerebbe quindi, per sua propria natura, dai limiti dell'art. 235. Essa può essere quindi realizzata unicamente mediante modifica del Trattato.* ».

Dall'altro lato, vi era la possibilità che la Comunità adottasse la propria Carta dei diritti fondamentali, affidando alla Corte di giustizia il potere di garantirne la corretta applicazione. In effetti fu proprio di questo secondo tipo la scelta adottata dal legislatore europeo.

I contenuti basilari della Carta sono stati dettati dalle conclusioni della riunione del Consiglio d'Europa tenutasi a Colonia nel 1999. In codesta sede si stabilì che la principale finalità della Carta era sensibilizzare maggiormente i cittadini dell'UE sull'importanza primaria e sulla pertinenza dei diritti fondamentali e che le principali fonti d'ispirazione a cui i redattori della Carta avrebbero dovuto fare riferimento sarebbero state in primis l'ordinamento CEDU e le tradizioni costituzionali comuni agli Stati membri, quali principi generali del diritto comunitario.

Per quel che concerne il diritto alla protezione dei dati personali, la Carta di Nizza risulta fondamentale poiché per la prima volta, su di un testo di carattere "costituzionale", avente valore generale e sovranazionale, era sancito il diritto alla protezione dei dati personali come diritto autonomo e distinto dal diritto alla riservatezza.

La Carta nello svolgimento del suo ruolo educativo-informativo nei confronti dei titolari dei diritti, degli Stati Membri, delle istituzioni e degli organismi europei contribuì in modo determinante, dal punto di vista giuridico, ad elevare il livello di protezione di quel diritto "all'autodeterminazione informativa", così come sancito anni prima dalla sentenza del BVerfG[25], che si innalzava definitivamente a valore costituzionale dell'ordinamento comunitario.

Infatti, nel capo secondo rubricato "*Libertà",* agli articoli 7 e 8 troviamo distinti rispettivamente: il rispetto della vita privata e familiare, che riprende pari passo il primo paragrafo dell'articolo 8 CEDU, e la protezione dei dati di carattere personale. L'articolo 8 recita quanto di seguito:

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 ottenere la rettifica.

[25] *Bundesverfassungsgericht,* Il Tribunale Costituzionale Federale Tedesco.

3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.

Come desumibile direttamente dal testo della norma vengono recepite tutte quelle innovazioni che, furono caratteristiche innovative delle legislazioni precedenti, partendo dalle prime leggi statali, passando per la Convenzione n.108/81, fino ad arrivare alla Direttiva 95/46/CE.

Vengono cristallizzati così, a livello costituzionale, i principi fondanti il diritto alla protezione dei dati personali come il principio di lealtà, delle finalità determinate del trattamento, il consenso della persona interessata, il diritto d'accesso ai propri dati da parte di quest'ultima e il diritto ad ottenerne la modifica e infine l'istituzione delle autorità garanti indipendenti deputate al controllo e lo sviluppo del diritto alla protezione dei dati sul territorio degli Stati Membri.

Determinante in quest'ambito risultò anche il Trattato di Lisbona firmato il 13 dicembre del 2007 che apportò modifiche sostanziali alla struttura dell'Unione Europea abolendo l'originaria suddivisione in tre pilastri e modificando i trattati istitutivi.

La modifica dei trattati fondanti l'UE era la strada alternativa tanto agognata per l'adesione alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, che grazie all'articolo 6, secondo paragrafo, del riformato Trattato UE, prevede che l'Unione aderisce alla Convenzione europea e che tale adesione non modifica le competenze dell'Unione come definite nei Trattati.

In questo modo è stata inserita la norma che offre la base legale per l'adesione dell'Unione alla CEDU; quella base legale, che la Corte UE aveva ritenuto allora inesistente nel suo parere n. 2/94[26].

[26] Bisogna rilevare come la Corte di Giustizia, su istanza della Commissione, con il parere 2/2013, ancora una volta, neghi la compatibilità con il diritto Ue della bozza di accordo di adesione dell'Unione Europea alla CEDU a causa di diversi problemi di armonizzazione tra i due sistemi di tutela soprattutto in ragione di una scarsa funzionalità di raccordo tra le due giurisdizioni. In sintesi l'UE fa perno sul ruolo del giudice comunitario, in contrapposizione all'idea della prevalenza di un'istanza giurisdizionale altra ed esterna come la CEDU, specialmente nell'ambito della tutela dei diritti fondamentali in relazione all'ambito d'applicazione del diritto UE. Il parere segna, dunque, una battuta di arresto rispetto alla lunga marcia verso l'adesione alla CEDU prevista dal Trattato di Lisbona. R. CALVANO, *Chi è la più bella del*

L'adesione alla Convenzione da parte dell'Unione è stata decisa contemporaneamente all'attribuzione formale di valore legale alla Carta dei diritti fondamentali dell'Unione, equiparato a quello dei Trattati[27], conferendole così carattere giuridico vincolante all'interno dell'ordinamento dell'Unione Europea.

6. Il panorama giuridico della protezione dati personali in Italia

All'interno della Costituzione Italiana non esiste un'esplicita disposizione che tuteli in modo diretto e autonomo la protezione dei dati personali dalla riservatezza in generale. Forse è meglio dire che all'epoca della nascita del testo costituzionale e per molto tempo dopo (più per una scelta linguistico–politica, che concettuale) i due concetti di riservatezza e protezione dei dati personali sono stati ricondotti nel più ampio ombrello della definizione di "Privacy".
Non a caso l'autorità indipendente di controllo, situata sul territorio italiano, è denominata "Garante della Privacy" e il Decreto Legislativo n. 196/2003, che detta e aggiorna la disciplina in tema di protezione dei dati personali in Italia, è comunemente chiamato "Codice della Privacy".
Riservatezza e Protezione Dati come due elementi complementari di un unico concetto di Privacy, a tutela della personalità e del suo libero sviluppo, tanto nell'intimità, quanto nella sua proiezione all'interno della società.
Perciò, più in generale, si ritenne confacente ad assicurare tale tutela il semplice riferimento, da un lato, a disposizioni costituzionali di carattere generale come gli articoli 2 e 3 della Costituzione, dall'altro, all'analisi di singole fattispecie la cui tutela è strettamente correlata con la protezione dati e la riservatezza (come gli articoli 13, 14, 15 e 21Cost.).

---

reame? Corte di Giustizia e Corte di Strasburgo alla luce del parere2/13 sull'adesione alla CEDU, in Diritto Pubblico Europeo Rassegna online, 2015.
[27] V. ZAGREBELSKY, *La prevista adesione dell'Unione Europea alla Convenzione europea dei diritti dell'uomo*, in www.europeanrights.eu/public/commenti/Adesione_Zagrebelsky.doc, 2007.

L’articolo 2 sancisce solennemente da parte della Repubblica Italiana l’assunzione del compito di riconoscere, di proteggere e di garantire i diritti inviolabili dell’uomo sia come singolo sia nelle formazione dove si sviluppa la sua personalità, sancendo il “principio personalista” come principio cardine della democraticità dell’ordinamento.

Al vertice della scala dei valori è riconosciuta la persona, per cui lo Stato è al servizio degli individui e non viceversa.

Sia a livello giurisprudenziale che dottrinale le tesi predominanti vedono nell'art. 2 della Costituzione una matrice generale di tutela del diritto alla privacy: la disposizione sembrerebbe pertanto fornire la “copertura costituzionale ai nuovi valori emergenti della personalità”[28].

Altre disposizioni costituzionali invece farebbero riferimento alla necessità di salvaguardare valori e libertà che possono essere pregiudicati dall'attività di trattamento dei dati personali come quelle dei seguenti articoli: l’articolo 13 che tutela la libertà della persona, l’articolo 14 che difende l’inviolabilità del domicilio, o come l’articolo 15 che protegge la segretezza delle comunicazioni e infine l’articolo 21 che difende la libera manifestazione del pensiero in tutte le sue forme.

In particolare, se consideriamo la privacy come aspetto legato alla libertà personale, tale diritto è riconosciuto come duplice libertà: da un lato come libertà negativa, che si definisce attraverso il concetto di “non interferenza altrui” nello spazio personale dell’individuo. Ad esso si riconduce l'aspetto negativo del diritto alla privacy, cioè la facoltà di trattenere nella propria sfera privata determinate informazioni; dall'altro come libertà positiva, che deve essere ricondotta ai concetti di potere e di controllo del proprio personale patrimonio informativo. Ciò riporta all'aspetto dinamico del diritto alla privacy, inteso come diritto di controllare la rivelazione e l'uso pubblico di dati, notizie e informazioni

[28] Si veda la sentenza della Corte costituzionale, 10 dicembre 1987, n. 479, inerente una controversia in tema di normativa sull’igiene del lavoro, nel quale la Corte ribadisce il “valore assoluto della persona umana sancito dall’articolo 2 Cost.”.

che siano attinenti alla propria persona e di agire autonomamente al fine di impedire lesioni.

Anche analizzando l'articolo 14 della Costituzione troviamo forti riscontri tra l'inviolabilità del proprio domicilio, concetto che richiama fortemente le garanzie del diritto di proprietà e la protezione della privacy.

L'articolo 14 Cost. tutela in maniera forte (con una riserva di legge e una riserva di giurisdizione) il domicilio da intrusioni dell'autorità di pubblica sicurezza ingiustificate e non fondate su di opportune previsioni derivanti dalla legge.

Secondo il profilo che a noi interessa, la ragione di una tutela così forte si giustifica poiché possiamo affermare che il domicilio indubbiamente rappresenti un "luogo privilegiato", nel quale la personalità umana può svolgere, senza interferenze esterne, ogni attività individuale e collettiva, essendo capace di offrire le condizioni per la piena e spontanea manifestazione della personalità dell'individuo.

Infine, la protezione della privacy rileva anche per quanto riguarda l'analisi delle dinamiche afferenti gli articoli 15 e 21 della Costituzione.

Il primo rileva come necessità della protezione della libertà e della segretezza della corrispondenza e più in generale delle comunicazioni, fenomeno che acquisisce sempre più importanza nell'era digitale, dove le forme di intromissione assumono forme sempre più evanescenti e invisibili.

Per quanto riguarda invece il diritto di informazione, racchiuso nell'articolo 21 della Costituzione, il concetto di privacy viene messo in rilievo principalmente sotto un duplice profilo: da un lato, il rapporto tra la libertà di informare, la tutela della persona e il diritto alla privacy; dall'altro, la possibilità di inquadrare la garanzia della libertà di manifestazione del pensiero e della stampa sotto il profilo del diritto di informare ed essere informati, dal quale derivano alcuni particolari limiti, individuabili nella rilevanza pubblico-sociale e nella verità obiettiva dei fatti riferiti, nel rispetto dell'altrui onore e reputazione, nella prevalenza di interessi di giustizia e della difesa nazionale e infine il rispetto dell'altrui riservatezza.

Per quanto riguarda, invece, la nascita di una vera e propria normativa settoriale sulla protezione dei dati personali, primo passo in tal senso fu fatto dalla Legge 300/1970 (c.d. Statuto dei Lavoratori).

Come precisa il giurista Stefano Rodotà nella sua analisi della trasformazione della privacy, da privilegio della classe borghese a conquista della classe operaia, la tutela della riservatezza diventa strumento per promuovere la parità di trattamento e realizzare l'eguaglianza tra cittadini, poiché i rischi politici connessi alle schedature di massa, in termini di discriminazione, intaccano specialmente le minoranze e la classe operaia rispetto le classi sociali più elevate[29].

Seguendo tale logica l'articolo 8 dello Statuto dei Lavoratori si presenta per l'epoca come una disposizione d'avanguardia nella parte in cui prevede che: «*È fatto divieto al datore di lavoro, ai fini dell'assunzione, come nel corso dello svolgimento del rapporto di lavoro, di effettuare indagini, anche a mezzo di terzi, sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore*.».

Veniva accordata così, al fine di prevenire ogni tipo di discriminazione all'interno del rapporto di lavoro, una protezione diretta alla categoria dei dati sensibili, ancor prima che in Italia si parlasse di un vero e proprio diritto alla protezione dei dati personali.

Soltanto a più di vent'anni di distanza venne introdotta una normativa a tutela della protezione dati, attuativa della Direttiva 95/46/CE, che nella sorte fu strettamente legata alla volontà dell'Italia di aderire alla Convenzione di Schengen.

Infatti condizione non negoziabile per i Paesi che volessero aderire a questa convenzione (che comportava l'abolizione delle barriere doganali anche rispetto

[29] S. RODOTA', *Tecnologie e diritti* , il Mulino, Bologna, 1995, p. 26.

alle persone oltre che per le merci) fu che essi adeguassero la propria legislazione ai principi e ai vincoli imposti dalla Direttiva 95/46[30].

L'Italia rispose a tale richiesta con la legge 31 dicembre 1996 n. 675 sulla "Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali".

Nel tempo furono emanate numerose altre normative, con l'intento di disciplinare i singoli e specifici aspetti del trattamento, nei diversi settori inerenti la protezione dati.

L'intento di specificazione e il frenetico sviluppo della disciplina portò al contrario ad un sovraffollamento normativo che contribuì a complicare non poco lo scenario del diritto alla protezione dati dell'epoca.

A quel punto fu sentita come un'esigenza indifferibile l'elaborazione di un Testo Unico, che raggruppasse i principi sulla protezione dei dati personali e al contempo disciplinasse e riordinasse la materia.

Così il 30 giugno 2003 fu emanato il Decreto Legislativo n.196 che istituisce il Codice in materia di protezione dei dati personali (anche detto Codice della Privacy) che razionalizza, semplifica e coordina in un unico testo tutte le precedenti disposizioni in Italia relative alla protezione dei dati personali.

Il Codice abroga la precedente Legge n.675/1996 dalla quale però, recepisce svariati principi e norme, e segnerà la normativa di riferimento fin quando il nuovo Regolamento Europeo n.679/2016, che riforma la materia, non entrerà in vigore e sarà applicato dal 25 maggio 2018 e ne modificherà l'impianto conformemente alle novità della disciplina.

[30] F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016, p. 67.

Capitolo II

La Regolamentazione Europea sulla Protezione dei Dati Personali: dalla Direttiva 95/46/CE al nuovo Regolamento UE 2016/679

Sezione I

Una rapida panoramica degli interventi normativi dell'Unione europea dalla Direttiva 95/46/CE fino al nuovo Pacchetto della Protezione Dati

1. La Direttiva "Madre" e le successive implementazioni: le Direttive 2002/58/CE e 2006/24/CE

La Direttiva Europea 95/46/CE segna un punto di svolta nel panorama normativo europeo in tema di protezione dei dati personali in quanto, per la prima volta, all'interno dell'Unione Europea, si richiedeva a tutti i Paesi di armonizzare le rispettive normative al fine di una più omogenea interpretazione e una più uniforme applicazione[31]. Non solo, l'intento riformatore doveva passare necessariamente, gradino per gradino, sulla "scala" di principi delineata dal testo normativo: principi minimi, ma tutti inderogabili. Principi come il consenso (libero, specifico e informato), il diritto d'accesso, di opposizione e di ottenere informazioni, i principi sul trasferimento dei dati oltrefrontiera, i principi sulla liceità del trattamento e sulla qualità dei dati nonché quelli sugli obblighi del

[31] Si prendano ad analisi i considerando 1 e 2 della Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati nella parte in cui affermano : « *che gli obiettivi della Comunità, enunciati nel trattato, come è stato modificato dal trattato sull'Unione europea, consistono nel realizzare un'unione sempre più stretta tra i popoli europei, nell'istituire relazioni più strette tra gli Stati che la Comunità riunisce, nell'assicurare mediante un'azione comune il progresso economico e sociale eliminando le barriere che dividono l'Europa, nel promuovere il miglioramento costante delle condizioni di vita delle sue popolazioni, nel preservare e rafforzare la pace e la libertà e nel promuovere la democrazia basandosi sui diritti fondamentali sanciti dalle costituzioni e dalle leggi degli Stati membri nonché dalla convenzione europea di salvaguardia dei diritti dell'uomo e delle libertà fondamentali.* » e di seguito: « *che i sistemi di trattamento dei dati sono al servizio dell'uomo; che essi, indipendentemente dalla nazionalità o dalla residenza delle persone fisiche, debbono rispettare le libertà e i diritti fondamentali delle stesse, in particolare la vita privata, e debbono contribuire al progresso economico e sociale, allo sviluppo degli scambi nonché al benessere degli individui.* ».

responsabile e dell'incaricato, entrano permanentemente nelle legislazioni nazionali diventando la base fondante del diritto alla protezione dei dati personali.

Come di frequente ammesso dai Garanti nazionali e dal Gruppo articolo 29, l'impianto semplice e agile ha fatto sì che la Direttiva risultasse un'eccellente "cassetta degli attrezzi"[32], capace di adattarsi a situazioni ed evoluzioni della materia diverse da quelle del momento in cui nasce. Tale semplicità di impianto però è stata anche uno dei punti deboli della normativa che sotto il peso schiacciante delle nuove tecnologie, specialmente quelle digitali, ha richiesto un innumerevole sforzo esegetico e analogico da parte della Corte di Giustizia Europea[33], delle Autorità Garanti Nazionali e infine del Gruppo di Lavoro ex articolo 29, al fine di adattare la normativa all'emergere dei nuovi fenomeni legati all'Internet e di imporre la salvaguardia dei principi in materia. Fondamentali a tal fine sono stati gli innumerevoli pareri del Gruppo, fin dai primi momenti della sua istituzione. Pareri che si evidenziano tanto per la tecnica giuridica adottata che per l'alto tasso di tecnicità utilizzata, richiedente un'ottima conoscenza del mondo digitale e dell'informatica[34].

L'opera del Gruppo ex articolo 29 è stata tanto preziosa quanto necessaria alla luce del fatto che, nonostante l'apporto integrativo delle successive legislazioni europee, come le Direttive 2002/58 e 2006/24[35], (rispettivamente in tema di telecomunicazioni elettroniche e in tema di comunicazioni elettroniche accessibili al pubblico o di reti pubbliche), non è bastato a coprire (e come

[32] Dichiarazione del Gruppo di lavoro ex Articolo 29 sul *Rafforzamento dell'ottemperanza dei responsabili del trattamento alla normativa sulla tutela dei dati* - WP101, Bruxelles, 2004.

[33] La giurisprudenza a riguardo è florida e di notevole fama basti solamente pensare ad esempio a CORTE DI GIUSTIZIA EUROPEA (grande sezione), 8 aprile 2014, Digital Rights Ireland Ltd (C-293/12) contro Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri,2014; CORTE DI GIUSTIZIA EUROPEA, causa C-131/12 *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González*, 2014; e CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), Sentenza nella causa C-362/14 Maximillian Schrems vsData Protection Commissioner, Lussemburgo, 6 ottobre 2015.

[34] Si pensi, solo per citarne alcuni, ai numerosi pareri del Gruppo Articolo 29 ad esempio sulle *anonymisation techniques* (WP216), sui *big data* (WP221), sui sistemi *cloud* (WP196), sulle *binding corporate rules* (WP195), sui *cookies* (WP194) e sull'*Internet of Things* (WP223).

[35] Modificativa della direttiva 2002/58 è stata poi abrogata dalla CGUE per difetto del principio di proporzionalità

avrebbe potuto data l'immensità dello spazio coperto e copribile dall'Internet) lo scarto generazionale che iniziava a dividere il diritto dall'emergente mondo del Web.

Costante e tenace è stato l'impegno profuso dal Gruppo che in questi anni è riuscito a coprire con le sue deliberazioni, il lungo margine di scarto che le nuove tecnologie hanno avanzato in tema di privacy e protezione dati, ma più in generale nella tutela dei diritti umani fondamentali.

Basti prendere ad esempio uno dei recenti pareri o lettere riguardante il caso Whatsapp - Facebook[36], per comprendere come sia effettivo e concreto l'approccio del Gruppo articolo 29 nella reale dialettica tra persone, Stati e grandi imprese nella tutela dei diritti. Non a caso, sempre più spesso, il diritto alla protezione dei dati personali è minacciato dall'azione, prevalentemente a fini commerciali, delle grandi aziende private e degli OTT[37].

Invero, questi grandi colossi commerciali che operano prevalentemente su di un terreno "digitalizzato", non rappresentano soltanto una minaccia, ma negli ultimi periodi e nelle vicende legate, nello specifico, agli attacchi terroristici degli ultimi tempi, si sono spesso e volentieri eretti a baluardo della difesa del diritto fondamentale alla protezione dei dati personali, contrastando richieste di ingerenza forzosa da parte delle autorità pubbliche di sicurezza, come accaduto in California, nel 2015 a seguito della strage di San Bernardino[38].

---

[36] Lettera WP29 a Facebook sul caso Whatsapp – 27/10/2016, dove il Gruppo pone sotto la lente d'ingrandimento alcune irregolarità derivanti dall'aggiornamento dei termini di servizio conseguenti all'all'acquisizione di Whatsapp da parte di Facebook: infatti il massiccio trasferimento delle informazioni riguardanti gli utenti dai server di Whatsapp su quelli di Facebook Inc. ha comportato alcune rilevanti violazioni dei principi della protezione dei dati personali tra cui quello del consenso e della finalità del trattamento, senza prevedere inoltre un adeguato sistema di controllo ed esercizio dei diritti per gli utenti. Testo consultabile su www.garanteprivacy.it

[37] Per *OTT* si intende l'acronimo di *Over-The-Top* , cioè le imprese che forniscono, attraverso la rete Internet, servizi, contenuti (soprattutto video) e applicazioni di tipo "rich media" (per esempio, le pubblicità che appaiono "sopra" la pagina di un sito web mentre lo si visita e che dopo una durata prefissata scompaiono). Esse traggono ricavo, in prevalenza, dalla vendita di contenuti e servizi agli utenti finali (ad esempio nel caso di Apple e del suo *iTunes*) o di spazi pubblicitari, come nel caso di Google e Facebook. Tali imprese, prive di una propria infrastruttura, agiscono "al di sopra delle reti", da cui il termine *Over-The-Top*. Cfr. AGCOM, relazione annuale, 2012.

[38] Si fa riferimento alla sparatoria avvenuta in un centro sociale per disabili a San Bernardino,in California, il 2 dicembre 2015 ad opera di Syed Rizwan Farook e Tashfeen Malik, marito e moglie, che aprirono il fuoco contro la folla, uccidendo all'istante 14 persone e ferendone altre 24, tra cui due poliziotti. Successivamente i due attentatori furono uccisi in uno scontro a fuoco con i poliziotti. Al di

Le problematiche riguardanti il caso Whatsapp – Facebook hanno avuto origine dalla acquisizione da parte della società di Mark Zuckerberg[39] del sistema di messaggistica istantanea più famoso al mondo (Whatsapp appunto), che ha unito così i due patrimoni informativi e di dati, in possesso delle due aziende più grandi al mondo operanti in questo settore.

Aldilà degli slogan del CEO[40] e co-fondatore di Whatsapp , Jan Koum[41], che tiene a rivendicare istanze indipendentistiche tra le due aziende, quantomeno nello svolgimento dei lavori, il problema allarmante alla base del disagio degli *users* delle due piattaforme multimediali è stata la modifica della *Privacy Policy* effettuata da Whatsapp a fine agosto del 2016.

Tale modifica dei termini generali riguardanti la protezione della privacy è stata il fattore decisivo affinché varie Autorità nazionali di controllo, tra cui il Garante per la Privacy tedesco e quello italiano, decidessero di avviare a tal proposito un'istruttoria al fine di determinare la correttezza delle nuove condizioni alle normative specifiche di settore. L'aggiornamento dei termini di servizio prevedeva la messa a disposizione di Facebook di alcune informazioni riguardanti gli account dei singoli utenti di Whatsapp, anche per finalità diverse da quelle "contrattuali" e riguardanti il settore *marketing* e *advertising*. A questo punto il Gruppo di Lavoro comune articolo 29[42] ha deciso di inoltrare una lettera

---

là dei fatti di cronaca la vicenda ebbe notevole risonanza anche a livello giuridico, a seguito della richiesta da parte dell'FBI rivolta alla Apple, sulla base dell'*obiter* del giudice federale del distretto centrale della California Sheri Pym, di creare un nuovo sistema operativo in grado di creare un accesso secondario (backdoor) al device così da poter prelevare tutto ciò che era all'interno dell'iPhone del terrorista. L'azienda Apple tuttavia non acconsentì alla richiesta dell'FBI motivando il rifiuto con la spiegazione che facendo acconsentendo alla richiesta si sarebbe potuto creare "precedente pericoloso", timore tra l'altro condiviso da altri giudici federali come James Orenstein (distretto di New York). Per un'analisi più approfondite del caso FBI-APPLE e dei risvolti critici per i diritti di libertà e protezione dei dati personali degli individui si rimanda a M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: dei diritti" violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 2016.

[39]Mark Zuckerberg è un dirigente d'azienda, imprenditore e informatico statunitense, fondatore del social network Facebook, di cui è amministratore delegato.

[40] *Chief Executive Officer* in inglese, è l'amministratore delegato di un'azienda.

[41]Jan Koum è un imprenditore e informatico statunitense nonché CEO e cofondatore di WhatsApp (insieme a Brian Acton), un'applicazione di messaggistica mobile che è stata di recente acquistata da Facebook Inc.

[42] Qui si ricorda che il Gruppo di Lavoro Comune ex articolo 29 è composto dall'insieme delle Autorità nazionali di controllo e protezione dati degli Stati dell'Unione e che si riunisce decidendo di comune accordo le politiche attuative dei principi derivanti dagli articoli 29 e 30 della Direttiva 95/46/CE.

al co-fondatore e CEO Jan Koum contenente l'invito a chiarire e fornire, date le numerose proteste degli utenti, tutti gli elementi utili alla valutazione del caso.

Nello specifico, il Gruppo lamentava le diverse finalità del trattamento dei dati che l'unione tra le due aziende avrebbe comportato (tra le quali appunto rientravano anche *marketing* e *advertising*): finalità che non erano incluse nella precedente informativa e che non furono accettate dagli utenti quando si iscrissero in un momento anteriore. Tutto ciò in contrapposizione anche alle precedenti dichiarazioni pubbliche delle due aziende che avevano assicurato che nessuna condivisione dei dati sarebbe mai avvenuta.

Inoltre, si paventavano rilevanti irregolarità riguardo le modalità con cui le informazioni relative all'aggiornamento dei termini di servizio e sulla privacy erano state fornite agli utenti, con serie preoccupazioni in merito alla validità del consenso di quest'ultimi, nonché del rispetto del principio di finalità.

Infine il Gruppo art. 29 metteva in dubbio anche l'efficacia dei meccanismi di controllo offerti agli utenti al fine dell'esercizio dei loro diritti e dei correlati effetti che la condivisione dei dati potrà avere sulle persone iscritte alle piattaforme multimediali di Facebook e Whatsapp.

Nello specifico però l'inquietudine maggiore era rivolta soprattutto a quella categorie di persone che, iscritte a Whatsapp, non erano però utenti di un qualsiasi altro servizio che rientrasse all'interno della *Facebook family of companies*[43] e per cui il trasferimento massiccio di dati, relativi agli account di questi soggetti, comportava un'irregolarità che non poggiava, in questo caso, nemmeno sul consenso dato per l'appartenenza ad entrambi i servizi multimediali.

Un tale intervento da parte del Gruppo e delle Autorità nazionali, singolarmente, ha fatto sì che in alcuni casi, come accaduto in Germania, direttamente dal semplice invio della richiesta di chiarimenti, potesse essere predisposta in maniera immediata la sospensione del flusso di dati da Whatsapp verso

[43] Tra le quali rientrano aziende produttrici di marchi e prodotti famosissimi sempre di natura tecnologico-informatica come Instagram, Facebook, Whatsapp, Oculus Rift e Private Core.

Facebook, affinché venisse prima accertata la conformità dell'operato delle due aziende rispetto alla normativa comunitaria esistente. Confortante in tal senso la risposta delle due multinazionali che si sono dichiarate pronte a collaborare e risolvere le eventuali incongruenze con la disciplina europea in tema di protezione dei dati personali.

Dunque risulta di immediata percezione l'importanza e la concretezza dell'operato del Gruppo articolo 29 e delle Autorità garanti nazionali che, tramite vie extragiudiziarie, sono capaci di intavolare dialoghi efficaci con i principali protagonisti dei vari settori afferenti la protezione dei dati personali al fine di prevenire controversie, risolvere conflitti e uniformare l'applicazione ai dettami dei principi fondanti la materia/disciplina.

Tornando all'analisi dello sviluppo della disciplina successiva all'emanazione della Direttiva "Madre" 95/46/CE, bisogna affermare anzitutto che l'apporto delle due Direttive comunitarie 2002/58 e 2006/24 è stato puramente integrativo e mai sostitutivo. Come sottolineato da autorevole dottrina[44] esse costituirono tanto un ampliamento quanto un rafforzamento del nucleo centrale della Direttiva Madre almeno per due ordini di ragioni: in primis poiché contengono molte norme integrative di un settore (quello delle telecomunicazioni e comunicazioni elettroniche) in cui la Direttiva 95/46 è decisamente carente; in secundis perché inglobando nelle nuove discipline l'intero apparato di controllo e vigilanza della Direttiva del '95 si è contribuito a rafforzarne e ampliarne funzioni, poteri e competenze[45].

Connotazione, quella integrativa, che si coglie chiaramente già in apertura all'articolo 1, paragrafo secondo, della Direttiva 2002/58/CE nella parte in cui specifica che: « *le disposizioni della presente Direttiva precisano e integrano la Direttiva 95/46/CE.*». Lo scopo principale è invece inquadrato al primo paragrafo

[44] F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016, p. 136.

[45] Art. 15 paragrafo 3 direttiva 2002/58 nella parte in cui dice «*Il Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'art. 29 della Direttiva 95/46, svolge i compiti di cui all'art. 30 della Direttiva stessa anche per quanto concerne materie disciplinate dalla presente Direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.*».

dell'articolo 1 che, indirettamente, ma non troppo, delinea anche il campo d'applicazione della nuova disciplina integrativa. Infatti risulta esplicito l'obiettivo che intende perseguire la normativa e cioè: proteggere i dati personali, con riguardo al trattamento di questi ultimi nel settore delle comunicazioni elettroniche, ma allo stesso tempo assicurare la circolazione di tali dati, delle apparecchiature e dei servizi di comunicazione elettronici all'interno della Comunità. Appare chiaro che il richiamo esplicito alla "Comunità" fa in modo di ricondurre la nuova disciplina all'interno del campo d'applicazione della Direttiva Madre, dunque, il primo pilastro. Intuizione confermata dal successivo paragrafo 3, che esplicitamente esclude l'applicazione della nuova direttiva nei campi non appartenenti alle attività ricomprese nel Trattato che istituisce la Comunità Europea, quali per esempio la sicurezza pubblica, la difesa e l'attività dello Stato, che siano inerenti al diritto penale, per citarne alcune.

Le novità non si rilevano solo dal punto di vista del settore disciplinato, quello appunto delle comunicazioni elettroniche, ma si riscontrano anche in alcune disposizioni cardine della direttiva che spostano l'attenzione direttamente sulla figura dell'utente dei servizi di comunicazione elettronica. Utente che per la prima volta si ritrova e si rapporta in uno scenario mutato rispetto al passato, dominato dall'Internet[46].

Compaiono, per la prima volta rispetto alle precedenti direttive sul tema della protezione dei dati personali, i riferimenti a spy-ware (i c.d. software spia), web bugs[47], cookies[48], reti mobili digitali e i dati relativi all'ubicazione[49], tutte nuove

[46] Considerando numero 6 " 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."

[47] Considerando n. 24 "identificatori occulti ed altri dispositivi analoghi che possono introdursi nel terminale dell'utente a sua insaputa al fine di avere accesso ad informazioni, archiviare informazioni occulte o seguire le attività dell'utente e possono costituire una grave intrusione nella vita privata di tale utente. L'uso di tali dispositivi dovrebbe essere consentito unicamente per scopi legittimi e l'utente interessato dovrebbe esserne a conoscenza."

[48] Considerando n.25 "i marcatori (c.d."cookies"), possono rappresentare uno strumento legittimo e utile, per esempio per l'analisi dell'efficacia della progettazione di siti web e della pubblicità, nonché per verificare l'identità di utenti che effettuano transazioni "on-line". Allorché tali dispositivi sono destinati a scopi legittimi, come facilitare la fornitura di servizi della società dell'informazione, il loro uso dovrebbe

tecnologie che nell'ambito delle comunicazioni sono state introdotte dalle novità della rete e che nel tempo hanno formato oggetto di numerose controversie e sono state al centro di numerosi pareri del Gruppo articolo 29.

Le disposizioni normative più significative della nuova disciplina sono sicuramente rappresentate dagli articoli 4 e seguenti, fino ad arrivare all'articolo 15 che chiude il cerchio affermando il principio di integrazione tra la Direttiva Madre del'95 la Direttiva n. 58 del 2002.

L'articolo 4 prende in analisi le misure di sicurezza prevedendo che il fornitore di un servizio di comunicazione elettronica accessibile al pubblico debba «*prendere appropriate misure tecniche e organizzative per salvaguardare la sicurezza dei suoi servizi, se necessario congiuntamente con il fornitore della rete pubblica di comunicazione per quanto riguarda la sicurezza della rete.*».

L'articolo 5 invece impone direttamente un obbligo in capo agli Stati mirato ad evitare che, per ragioni diverse dalla fornitura del servizio, l'autorità pubblica possa usufruire dei canali creati e creabili dalle comunicazioni elettroniche, tramite la rete internet, al fine di esercitare un controllo di massa e indiscriminato

---

essere consentito purché siano fornite agli utenti informazioni chiare e precise, a norma della direttiva 95/46/CE, sugli scopi dei marcatori o di dispositivi analoghi per assicurare che gli utenti siano a conoscenza delle informazioni registrate sull'apparecchiatura terminale che stanno utilizzando. Gli utenti dovrebbero avere la possibilità di rifiutare che un marcatore o un dispositivo analogo sia installato nella loro apparecchiatura terminale. Ciò riveste particolare importanza qualora utenti diversi dall'utente originario abbiano accesso alle apparecchiature terminali e quindi a dati contenenti informazioni sensibili in relazione alla vita privata che sono contenuti in tali apparecchiature. L'offerta di informazioni e del diritto di opporsi può essere fornita una sola volta per l'uso dei vari dispositivi da installare sull'attrezzatura terminale dell'utente durante la stessa connessione e applicarsi anche a tutti gli usi successivi, che possono essere fatti, di tali dispositivi durante successive connessioni. Le modalità di comunicazione delle informazioni, dell'offerta del diritto al rifiuto o della richiesta del consenso dovrebbero essere il più possibile chiare e comprensibili. L'accesso al contenuto di un sito Internet specifico può tuttavia continuare ad essere subordinato all'accettazione in conoscenza di causa di un marcatore o di un dispositivo analogo, se utilizzato per scopi legittimi."

[49] Considerando n. 35 " Nelle reti mobili digitali i dati relativi all'ubicazione, che consentono di determinare la posizione geografica dell'apparecchiatura terminale dell'utente mobile vengono sottoposti a trattamento in modo da consentire la trasmissione di comunicazioni. Tali dati sono quelli relativi al traffico di cui all'articolo 6 della presente direttiva. Tuttavia, in aggiunta ad essi, le reti mobili digitali possono avere la capacità di trattare dati relativi all'ubicazione che possiedono un grado di precisione molto maggiore di quello necessario per la trasmissione delle comunicazioni e che vengono utilizzati per fornire servizi a valore aggiunto, come i servizi che forniscono informazioni individuali sul traffico e radioguida. Il trattamento di dati siffatti ai fini della fornitura di servizi a valore aggiunto dovrebbe essere autorizzato soltanto previo esplicito consenso dell'abbonato. Anche in questo caso, tuttavia, gli abbonati dovrebbero disporre, gratuitamente, di un mezzo semplice per bloccare temporaneamente il trattamento dei dati relativi alla loro ubicazione".

capace di ledere pesantemente la riservatezza della persona, così come accaduto in passato[50]. È fatto espresso divieto di procedere all'«*ascolto, la captazione, la memorizzazione e altre forme di intercettazione o di sorveglianza delle comunicazioni, e dei relativi dati sul traffico, ad opera di persone diverse dagli utenti, senza consenso di questi ultimi, eccetto quando sia autorizzato legalmente a norma dell'articolo 15, paragrafo 1. Questo paragrafo non impedisce la memorizzazione tecnica necessaria alla trasmissione della comunicazione fatto salvo il principio della riservatezza.*». Ovviamente tale divieto non opera per le motivazioni di cui all'articolo 15, par.1[51] e in quei casi in cui la registrazione sia effettuata nel quadro di legittime prassi commerciali al fine di fornire la prova di una transazione o di una qualsiasi comunicazione commerciale[52].

Il paragrafo 3 sottolinea l'importanza dell'informativa da rivolgere all'utente.

Infatti è fatto obbligo agli Stati Membri di assicurare che l'utilizzo delle reti di comunicazione elettronica, ai fini di archiviazione di informazioni o di accesso ad informazioni archiviate nell'apparecchio terminale dell'utente, possa essere eseguito legittimamente "*unicamente a condizione che*" il soggetto sia stato informato in modo "*chiaro e completo*" sugli scopi del trattamento e che gli sia offerta, inoltre, la possibilità di rifiutare tale trattamento[53].

È questa a tutti gli effetti una delle disposizioni centrali della disciplina e che svolge un ruolo importantissimo al fine di ribadire la centralità dell'utente e della necessità di un suo consenso informato, come garanzia a fronte di intrusioni illecite.

---

[50] Si rimanda ancora una volta all'attenta analisi storica sulla nascita della protezione dati come diritto fondamentale di libertà inteso come difesa dal controllo di massa sulle persone perpetrato dagli Stati autoritario del primo '900. F. PIZZETTI, *La privacy e il diritto…*, cit., p. 50-53.

[51] Nella parte in cui prevede che "tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica."

[52] Articolo 15 paragrafo 2

[53] A tal proposito in tema di *cookies* si rimanda a GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies*, doc. web n. 311884, 8 maggio 2014.

Proseguendo nell'analisi delle disposizioni più importanti figurano a seguire gli articoli 6 e 7: il primo predispone la cancellazione e la anonimizzazione[54] dei dati di traffico qualora, questi ultimi, non siano più necessari ai fini della trasmissione delle comunicazioni; mentre il secondo stabilisce il principio per cui gli utenti hanno diritto a ricevere fatture dettagliate, lasciando il compiti ai rispettivi Stati Membri di decidere le modalità più funzionali al rispetto della vita privata.

In aggiunta l'articolo 9 tocca un tema di grande importanza, rilevante anche al giorno d'oggi: i dati che trasmettono informazioni relative all'ubicazione della comunicazione, aventi di per sé grandi capacità di localizzazione[55].

I dati relativi all'ubicazione sono quei dati che possiedono un alto grado di precisione e che sono capaci di individuare la posizione geografica dell'apparecchio utilizzato dall'utente. Capacità di gran lunga superiore rispetto a quella necessaria per la trasmissione delle comunicazioni. Perciò è previsto, quale condizione indispensabile per il loro utilizzo, che codesti dati « *siano stati resi anonimi o che l'utente o l'abbonato abbiano dato il loro consenso, e sempre nella misura e per la durata necessaria per la fornitura di un servizio a valore aggiunto*[56]. ».

Infine l'importanza dell'articolo 15 risiede principalmente nel fatto che i richiami operati all'interno della disposizione creano un ponte diretto tra il nocciolo duro della vecchia disciplina e il nuovo contesto operativo delineato dalla recente

---

[54] Per il Gruppo articolo 29 i dati anonimi sono quei dati "*privati di elementi sufficienti per impedire l'identificazione della persona interessata. Più precisamente, i dati devono essere trattati in maniera tale da non poter più essere utilizzati per identificare una persona fisica utilizzando "l'insieme dei mezzi che possono essere ragionevolmente utilizzati" dal responsabile del trattamento o da altri. Un fattore importante è che il trattamento deve essere irreversibile.*". GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 "sulle tecniche di anonimizzazione" (WP 216), 10 aprile 2014.

[55] In tema GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 13/2011 *sui servizi di geolocalizzazione su dispositivi mobili intelligenti*, (WP185), 16 maggio 2011.

[56] *Servizio a Valore Aggiunto* (*VAS*, acronimo di *Value-Added Service*) è un termine tipico dell'industria di telecomunicazioni che indica tutti i servizi al di fuori dei servizi di base, ovvero delle chiamate di voce standard e delle trasmissioni fax. Tale terminologia si è estesa nel tempo ad altri settori economici. Nell'industria delle telecomunicazioni i servizi a valore aggiunto aumentano il valore dell'offerta di servizio standard spronando l'abbonato ad usare di più il loro telefono e permettendo all'operatore di ottimizzare il guadagno medio per utente (ARPU). Nella telefonia mobile le tecnologie quali sms, mms e GPRS generalmente sono considerate tra i servizi a valore aggiunto.

Direttiva. Ciò avviene, in un primo momento, tramite il richiamo dell'articolo 13 paragrafo 1 della Direttiva 95/46, per cui gli Stati possono limitare i diritti e gli obblighi sanciti nella Direttiva 2002/58 solamente se tale restrizione costituisce «*una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica.*»; successivamente, sancendo la piena sovrapposizione degli stessi compiti, elencati nell'articolo 30 della Direttiva 95/46, del Gruppo di Lavoro ex art.29 anche alla materia delle comunicazioni elettroniche previste dalla Direttiva del 2002.
In tal modo si è voluto creare un sistema normativo coordinato e complementare, anzi come detto in precedenza integrativo e aggiuntivo, mai sostitutivo della base di principi enucleati nella Direttiva Madre.

2. La Direttiva 2006/24/CE: l'esigenza di una disciplina comune sulla conservazione dei dati e la successiva invalidità proclamata dalla Corte di Giustizia Europea

La Direttiva 2006/24/CE del Parlamento Europeo e del Consiglio 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* », non ha avuto una vita molto lunga nonostante fosse incentrata su di una tematica molto importante e profondamente sentita all'interno del contesto della protezione dei dati personali: la conservazione, memorizzazione e il successivo utilizzo del dato.
Infatti la c.d. Direttiva "*Frattini*[57]" o "*Data Retention*", diversamente dagli altri due impianti normativi (Dir. 95/46 e Dir 2002/58), imposta il fulcro della sua

[57] Prende infatti il nome dall'allora Vicepresidente e Commissario per la Giustizia e gli Affari Interni, Franco Frattini, che fortemente ne ha voluto l'emanazione.

disciplina sempre nell'ambito della protezione dei dati personali nelle comunicazioni elettroniche, ma concentrandosi sull'aspetto della « *conservazione e del loro uso per finalità di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato Membro nella propria legislazione nazionale.* », inteso come obbligo facente capo ai fornitori dei servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione. Invece il campo d'applicazione della normativa è individuato nei dati relativi al traffico e all'ubicazione delle persone, sia fisiche che giuridiche, nonché ai dati necessari per identificare l'abbonato o l'utente registrato.

Nonostante il carattere innovativo e al tempo stesso sostitutivo della meno recente Direttiva 2002/58, la Direttiva "*Data-Retention*" richiama esplicitamente, al primo paragrafo dell'articolo 2, le definizioni contenute nella Direttiva Madre del '95 (sono incluse nel richiamo anche la Direttiva 2002/58/CE e la Direttiva 2002/21/CE[58]) a voler sottolineare ancora una volta, come già affermato nel paragrafo precedente, il carattere integrativo delle nuove discipline, della loro funzione di aggiornamento, però mai sostitutivo della disciplina "base". Anzi a tal proposito uno degli obiettivi principali della Direttiva è proprio quello di tradurre i principi enunciati dalla Direttiva Madre in norme specifiche per il settore delle comunicazioni elettroniche[59]. La necessità dell'adozione di una più stringente ed efficace normativa, comune a livello europeo, sulla conservazione dei dati di traffico delle comunicazioni elettroniche, si fece più pressante specialmente a seguito degli attacchi terroristici di Londra avvenuti nel 2005[60]. Gli attacchi terroristici, che furono rivendicati anche dalla rete jihadista di Al Qaeda, crearono un fortissimo senso di instabilità e preoccupazione nella capitale

[58] Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce "*un quadro normativo armonizzato per la disciplina dei servizi di comunicazione elettronica, delle reti di comunicazione elettronica e delle risorse e servizi correlati, definisce le funzioni delle autorità nazionali di regolamentazione ed istituisce le procedure atte a garantire l'applicazione armonizzata del quadro normativo nella Comunità."* (articolo 1).

[59] Come da considerando n.2

[60] Come anche riportato nel considerando n.10 per cui "*Il 13 luglio 2005 il Consiglio ha ribadito nella sua dichiarazione di condanna degli attacchi terroristici di Londra la necessità di adottare al più presto misure comuni in materia di conservazione dei dati relativi alle telecomunicazioni*."

inglese all'alba della conferma della scelta di Londra come città che avrebbe ospitato le prossime Olimpiadi.

In una città violata nel giro di pochissime ore da quattro diverse esplosioni, tutte dettagliatamente coordinate fra loro (tre su diverse linee della metropolitana e una all'interno di un autobus a due piani diretto in centro), e che causarono ben 57 vittime, l'esigenza di una pronta risposta da parte della nazione e degli apparati di sicurezza, spesso e volentieri, può portare a gravi e consistenti violazioni dei diritti individuali, specialmente di quelli afferenti l'area della privacy e della protezione dei dati personali.

Stante dunque la diversità d'impianto delle varie normative degli Stati Membri in materia, riscontrata inoltre la grande utilità della conservazione dei dati come strumento di contrasto e di prevenzione effettivo rispetto a gravi reati come quelli di terrorismo e di criminalità organizzata, l'armonizzazione delle differenti leggi sul territorio dell'Unione, nella direzione della creazione di una disciplina comune, risultava essere un impegno improrogabile.

Impegno, non solo mirato alla predisposizione di una disciplina effettiva che regolasse la conservazione dei dati per i fini di indagine e prevenzione dei reati di terrorismo, ma orientato anche ad evitare che situazioni di gravi crisi legate alla sicurezza nazionale potessero essere veicoli, per gli apparati di pubblica sicurezza, attraverso i quali oltrepassare e calpestare quei limiti imposti dall'osservanza e il rispetto dei diritti fondamentali dell'uomo così come sanciti dalle convenzioni e dalle carte internazionali ed europee.

A tal fine si imponeva oltre a una lettura garantista, orientata al rispetto dei requisiti mutuati dall'articolo 8 CEDU, dai principi della Convenzione n. 108/1981 e dalle precedenti Direttive Europee, anche la necessità di ancorare la tutela dei dati personali entro rigidi intervalli temporali.

Ciò in ragione del fatto che in situazioni di gravi emergenza, come quelle conseguenti ad un attacco terroristico su territorio nazionale, i governi degli Stati Membri possono/potrebbero cedere alle forti pressioni degli apparati di sicurezza determinando così un allungamento irragionevole e sproporzionato dei tempi di

conservazione, tale da pregiudicare i diritti delle persone che utilizzano mezzi di comunicazione elettronica.

La disposizione centrale della Direttiva 2006/24/CE che illustra tassativamente il periodo minimo e massimo di conservazione dei dati, e che è stata la causa principale dell'annullamento ad opera della famosa sentenza *Digital Rights Ireland* della Corte di Giustizia Europea, è rappresentata dall'articolo 6 che così recita: «*Gli Stati membri provvedono affinché le categorie di dati di cui all'articolo 5*[61] *siano conservate per periodi non inferiori a sei mesi e non superiori a due anni dalla data della comunicazione.*».

[61] L'articolo 5 contiene un lungo elenco di categorie di dati legati al settore delle comunicazioni elettroniche, qui si richiama integralmente il contenuto dell'articolo 5 rubricato "Categorie di Dati da conservare":

«1. *Gli Stati membri provvedono affinché in applicazione della presente direttiva siano conservate le seguenti categorie di dati:*

a) i dati necessari per rintracciare e identificare la fonte di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

i. numero telefonico chiamante;

ii. nome e indirizzo dell'abbonato o dell'utente registrato;

2) per l'accesso Internet, posta elettronica su Internet e telefonia via Internet:

i. identificativo/i dell'utente

ii. identificativo dell'utente e numero telefonico assegnati a ogni comunicazione sulla rete telefonica pubblica;

iii. nome e indirizzo dell'abbonato o dell'utente registrato a cui al momento della comunicazione sono stati assegnati l'indirizzo di protocollo Internet (IP), un identificativo di utente o un numero telefonico;

b) i dati necessari per rintracciare e identificare la destinazione di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile:

i. numero/i digitato/i (il numero o i numeri chiamati) e, nei casi che comportano servizi supplementari come l'inoltro o il trasferimento di chiamata, il numero o i numeri a cui la chiamata è trasmessa;

ii. nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i;

2) per la posta elettronica su Internet e la telefonia via Internet:

i. identificativo dell'utente o numero telefonico del/dei presunto/i destinatario/i di una chiamata telefonica via Internet;

ii. nome/i e indirizzo/i dell'abbonato/i o dell'utente/i registrato/i e identificativo del presunto destinatario della comunicazione;

La Corte in primis rileva come le categorie di dati illustrate dall'articolo 5, anche se non attingono direttamente al contenuto della conversazione, siano comunque in grado di fornire informazioni importanti sulle comunicazioni, sui loro destinatari e sulla loro frequenza. Pertanto l'accesso a tali dati, da parte dell'autorità pubblica, comporta in ogni caso una seria ingerenza nella vita privata dei cittadini, ingenerando peraltro in loro l'idea di essere esposti a una

---

c) i dati necessari per determinare la data, l'ora e la durata di una comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile, data e ora dell'inizio e della fine della comunicazione;

2) per l'accesso Internet, la posta elettronica via Internet e la telefonia via Internet:

i. data e ora del log-in e del log-off del servizio di accesso Internet sulla base di un determinato fuso orario, unitamente all'indirizzo IP, dinamico o statico, assegnato dal fornitore di accesso Internet a una comunicazione e l'identificativo dell'abbonato o dell'utente registrato;

ii. data e ora del log-in e del log-off del servizio di posta elettronica su Internet o del servizio di telefonia via Internet sulla base di un determinato fuso orario;

d) i dati necessari per determinare il tipo di comunicazione:

1) per la telefonia di rete fissa e la telefonia mobile: il servizio telefonico utilizzato;

2) per la posta elettronica Internet e la telefonia Internet: il servizio Internet utilizzato;

e) i dati necessari per determinare le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature:

1) per la telefonia di rete fissa, numeri telefonici chiamanti e chiamati;

2) per la telefonia mobile:

i. numeri telefonici chiamanti e chiamati;

ii. International Mobile Subscriber Identity (IMSI) del chiamante;

iii. International Mobile Equipment Identity (IMEI) del chiamante;

iv. l'IMSI del chiamato;

v. l'IMEI del chiamato;

vi. nel caso dei servizi prepagati anonimi, la data e l'ora dell'attivazione iniziale della carta e l'etichetta di ubicazione (Cell ID) dalla quale è stata effettuata l'attivazione;

3) per l'accesso Internet, la posta elettronica su Internet e la telefonia via Internet:

i. numero telefonico chiamante per l'accesso commutato (dial-up access);

ii. digital subscriber line (DSL) o un altro identificatore finale di chi è all'origine della comunicazione;

f) i dati necessari per determinare l'ubicazione delle apparecchiature di comunicazione mobile:

1) etichetta di ubicazione (Cell ID) all'inizio della comunicazione;

2) dati per identificare l'ubicazione geografica delle cellule facendo riferimento alle loro etichette di ubicazione (Cell ID) nel periodo in cui vengono conservati i dati sulle comunicazioni.

2. A norma della presente direttiva, non può essere conservato alcun dato relativo al contenuto della comunicazione. ».

"costante sorveglianza" in quanto la conservazione e il successivo utilizzo dei dati stessi avviene a insaputa dell'interessato[62].

Successivamente passa allo scrutinio della disposizione riguardante i termini di conservazione dei dati e che secondo il parere della Corte sarebbe il principale motivo alla base dell'annullamento della Direttiva "*Data Retention*".

Infatti la principale accusa mossa all'articolo 6 consisterebbe nella violazione, da parte della disposizione, del principio di stretta proporzionalità, per la quale sarebbe sorto un connaturale contrasto con il diritto fondamentale alla protezione dei dati personali così come definito dalla normativa comune europea.

La Corte dunque ha elaborato cinque ordini di motivi, posti alla base della decisione di annullamento della Direttiva:

1) aver previsto termini indifferenziati e generalizzati all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta ai reati gravi;
2) aver omesso ogni criterio che consenta di definire quando i reati possano essere considerati sufficientemente gravi da giustificare una simile ingerenza;
3) aver omesso ogni presupposto procedurale e sostanziale al quale subordinare l'accesso;
4) aver omesso ogni criterio per differenziare la durata della conservazione dei dati, limitandosi solo a stabilire i termini minimi e massimi;
5) aver omesso di imporre che i dati acquisiti debbano essere conservati esclusivamente nel territorio dell'Unione.

Dunque secondo il parere della Corte dell'8 aprile 2014[63], che ha sancito l'invalidità della Direttiva "*Data Retention*", un grave difetto è stata la mancanza

[62] Si veda "*Intervento di Antonello Soro, Presidente del Garante per la protezione dei dati personali-L'Huffington Post", 8 aprile 2014* sulla sentenza della corte di giustizia sulla sentenza data retention, facilmente visionabile in www.garanteprivacy.it .

[63] CORTE DI GIUSTIZIA EUROPEA (grande sezione), 8 aprile 2014, Digital Rights Ireland Ltd (C-293/12) contro Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri,2014.

di specificazione e differenziazione normativa, specialmente in una materia (quella della protezione dei dati personali) in cui il rischio di generalizzazione può incidere gravemente nella sfera privata dei cittadini.

Non solo, l'esigenza di specificazione è ancora più sentita in un settore, quale quello del contrasto al crimine, in cui maggiori sono le limitazioni alle libertà, ammesse per esigenze di interesse generale e che possono derivare in un controllo indifferenziato di massa, tramite la raccolta generalizzata e l'utilizzo dei dati relativi alle comunicazioni elettroniche.

Il punto cardine della pronuncia è indubbiamente il principio di stretta proporzionalità tra limitazioni dei diritti fondamentali ed esigenze di pubblica sicurezza: proporzionalità che non va delineata solamente in astratto e in maniera indifferenziata rispetto a qualsiasi reato ma che, al contrario, esige una differenziazione attenta e modulata in base al tipo di delitto, alle esigenze investigative, al tipo di dato e di mezzo di comunicazione utilizzato[64].

3. Il Regolamento UE 2016/679 e le differenze con la Direttiva "Madre": una rapida panoramica

Ad una prima e rapida lettura sono molte le innovazioni e le differenze tra il vecchio apparato normativo e il nuovo Regolamento europeo che è entrato in vigore nel mese di maggio 2016 (a seguito dei canonici venti giorni dalla pubblicazione nella *Gazzetta ufficiale dell'Unione Europea*), ma la sua applicazione decorrerà formalmente dal 25 maggio 2018[65]. Un arco temporale di due anni, utile affinché gli Stati Membri abbiano la possibilità di organizzare al meglio l'impianto normativo nazionale in modo tale da inserire efficacemente il Regolamento all'interno del proprio ordinamento. Una preparazione che dovrà essere attenta ed efficiente in quanto la prima differenza tra la nuova e la vecchia

[64] *Ibidem*.

[65] Come precisato nel Capo XI dedicato alle "*Disposizioni Finali*", dove all'articolo 99 è previsto che "*Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella Gazzetta ufficiale dell'Unione europea*", ma che quest'ultimo "*si applica a decorrere da 25 maggio 2018*".

disciplina in tema di protezione dei dati personali si riscontra proprio nel mezzo mediante il quale quest'ultima è introdotta: il Regolamento.

Non più dunque una Direttiva d'armonizzazione che cerca, tramite l'azione degli Stati Membri, di riavvicinare il più possibile normative e culture giuridiche, a volte molto diverse tra loro, ma uno strumento giuridico forte avente carattere vincolante e come tale, obbligatorio in tutte le sue parti e direttamente applicabile in tutti gli Stati Membri dell'Unione Europea.

L'obiettivo principe del Regolamento non è soltanto quello di introdurre una nuova e più robusta disciplina per la protezione dei dati personali, sostitutiva della Direttiva 95/46/CE, che sia applicata in maniera conforme e uniforme in tutto il territorio dell'Unione, ma specialmente quello di creare un ponte tra il passato, il presente e il futuro della materia. Un ponte dove i principi enucleati nella Direttiva Madre costituiscono le salde fondamenta e i pilastri portanti, dove l'immensa opera giurisprudenziale insieme al prezioso lavoro dei Garanti nazionali e del Gruppo di Lavoro Comune ex articolo 29, tramite i suoi numerosi pareri, costituiscono una struttura salda e "cementata" e dove, infine, il Regolamento si presenta come la "passerella", il cammino che partendo dalle conquiste del passato si evolve e unisce il presente, ma soprattutto guarda al futuro.

Dunque un cammino quello intrapreso che non disconosce il passato, anzi da quello stesso passato trae origine e forza vitale, proiettandosi però inesorabilmente verso il futuro e, con l'intenzione di rivoluzionare il presente, cambia in modo determinante tanto la concezione quanto l'approccio giuridico, ma anche sociale, alla protezione dei dati personali.

Così facendo il Regolamento non innova solamente la materia tramite l'introduzione di istituti completamente nuovi[66], facendosi interprete delle problematiche più pressanti della società digitale moderna, ma attua un lavoro di

[66] Si pensi alle grandissime innovazioni, volendo citarne solo alcune, introdotte dal Regolamento UE/2016/679 tra cui la figura del Data Protection Officer (il responsabile della protezione dei dati personali), il diritto all'oblio e alla portabilità dei dati, la *privacy by design and by default*, la valutazione pre-impatto e la consultazione preventiva, gli obblighi e le misure di sicurezza riguardo la *data breach*.

consolidamento di tutte quelle posizioni e determinazioni che in questi anni hanno costituito il lavoro del Gruppo art.29 e della giurisprudenza della Corte di Giustizia europea, e infine conferma, amplia e aggiorna il *set of principles* derivante dalla Direttiva del '95, dettando una disciplina puntuale, chiara e il più possibile votata a soddisfare esigenze di completezza dei contenuti, così come richiede l'impianto normativo di un atto *self executing* come un regolamento europeo.

Nonostante gli innegabili profili di novità introdotti dalla recente normativa comunitaria non sono mancate posizioni, quantomeno dubbiose, riguardo la concreta operabilità del Regolamento e di alcune scelte del legislatore europeo. Alcuni autori, come il professor Franco Pizzetti, nutrono timori sulla tecnica normativa utilizzata da parte del legislatore europeo secondo cui in alcune parti del testo, data la voluta generalità, sembrerebbe esporre il fianco a interpretazioni della stessa disposizione anche molto diverse tra loro, in altre parti invece a causa del carattere rigido di alcune norme («*da apparire più come affermazioni di principio che come dettati normativi*[67]») sembra essere così limitativa da far figurare la protezione dati predisposta dal Regolamento addirittura indebolita rispetto al sistema di tutela più flessibile della Direttiva.

Non solo, ulteriori preoccupazioni deriverebbero dal fatto che, in tema di definizioni relative ai principi e ai concetti principali della materia, una «*maniacale vocazione al dettaglio*» potrebbe essere causa di un eccessivo irrigidimento e un prematuro invecchiamento della normativa. Volendo usare le parole di Franco Pizzetti si corre il rischio di «*regolare il futuro con la testa girata all'indietro*». A parte i leciti timori che porta con sé un "Pacchetto normativo[68]" come quello della Protezione Dati, molto sentito nell'ambiente giuridico, data la delicatezza del settore nel quale la protezione opera, bisogna

[67] F. PIZZETTI, *La privacy e il diritto…,* cit., p. 150.

[68] Si ricorda che il Pacchetto Protezione Dati è composto oltre che dal Regolamento n. 679/2016, anche dalla Direttiva n. 680/2016 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio.".*

scendere a patti necessariamente con la forma utilizzata dal legislatore europeo (e Franco Pizzetti sembra comprendere con grandissima e lodevole visione d'insieme il perché della necessità, nonostante talune perplessità, dell'utilizzo del Regolamento come risposta alle carenze del precedente sistema normativo).

Infatti la scelta della forma regolamentare ha precise ragioni che trovano la loro genesi proprio nelle mancanze che la Direttiva Madre ha rivelato nel tempo.

Numerose volte si è lodata l'elasticità della tecnica legislativa adottata nella Direttiva Madre capace di assumere svariate "vesti" tutte molto funzionali a seconda della situazione che si trovava a dover fronteggiare, un'utilissima "cassetta degli attrezzi" dotata di una interoperabilità che è stata fondamentale nella risoluzione di problematiche, al tempo dell'adozione della Direttiva, neppure immaginabili.

Proprio questa camaleontica possibilità d'utilizzo, che si rispecchia specialmente nella compattezza, sinteticità e semplicità utilizzata nel delineare e definire concetti e principi, è stata la prima causa di una non poco problematica differenziazione normativa in tutto il territorio dell'Unione, che è stata poi alla base della scelta dell'adozione di un regolamento che avrebbe garantito così maggiore uniformità.

Invero il Regolamento sembra voler ricercare un punto di equilibrio, un giusto compromesso, tra generalità e semplicità di impianto in modo tale da garantire in determinate situazioni un'apprezzabile elasticità di interpretazione, con lo scopo di fronteggiare al meglio questioni che potrebbero verificarsi in futuro e che possono apparire al momento non ancora prevedibili (ipotesi questa che, come si è visto, si verifica non di rado quando si parla di tecnologie legate al web), e una cura nel dettaglio durante la redazione di definizioni e principi che mira alla creazione di un nucleo centrale di nozioni, tassativo e granitico, quasi una sorta di "Statuto del Diritto alla Protezione Dati" che nel suo contenuto, nei suoi principi e definizioni non può e non deve essere manipolato dagli Stati Membri ovvero essere soggetto a diverse interpretazioni.

In effetti appare una strategia legislativa, dati i presupposti, convincente: poiché utilizzando le parole di Salvatore Sica: «*poche materie come questa necessitano di un difficile mix tra definizioni legislative "elastiche" e, ove occorra, di interventi regolamentari di dettaglio*[69]. ».

Ciò che si nota da un primo raffronto tra il Regolamento 2016/679/UE e la Direttiva 95/46/CE è sicuramente la maggiore estensione della struttura del primo rispetto la seconda. La maggiore attenzione al dettaglio e alla specificazione predisposta dal legislatore europeo ha fatto sì che si partorisse una struttura normativa del Regolamento molto ampia che arriva a contare ben undici capi, composti anche da più sezioni l'uno, e ben novantanove articoli. La differenza con la Direttiva, che al contrario conta soltanto sette capi e trentaquattro articoli (nemmeno un terzo di quelli che compongono il Regolamento), è immediatamente percepibile.

Ancora una volta la soluzione può essere ricercata nella diversità di scopi ai quali i due strumenti normativi sono deputati: la Direttiva aveva la necessità di configurarsi come uno strumento agile e snello, che fungesse da linea guida per l'armonizzazione delle legislazioni nazionali, che sarebbe poi avvenuta ad opera degli Stati Membri; mentre il Regolamento, essendo un atto normativo *self executing* e obbligatorio in tutte le sue parti, richiede una maggiore completezza e chiarezza di contenuti, disciplinando nella maniera più precisa possibile gli istituti di cui è composto.

In questo binomio costante tra la volontà di rendere la disciplina, alcune volte, il più elastica possibile, altre volte, incanalarla nei rigidi binari di un estrema specificità, il Regolamento inevitabilmente risente in modo molto forte della Direttiva, ad esempio nella formulazione di alcune norme che si presentano quasi come una perfetta riproduzione[70], mentre in altri parti del testo normativo si

[69] S. SICA, *Verso l'unificazione del diritto europeo alla tutela dei dati personali?,* Cap. I, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 5.

[70] Si mettano a confronto per esempio la Direttiva all'art. 3 par. 1 e il nuovo Regolamento all'art. 2 par. 1, che disciplinano entrambi l'ambito di applicazione della normativa. Le due disposizioni sono l'una la ripetizione dell'altra dal momento che entrambe delimitano il campo d'applicazione nel "*trattamento*

distacca in maniera così netta da costituire un totale rovesciamento rispetto alle posizioni sancite nella Direttiva del '95.

Un esempio, a tal proposito, lo si riscontra già attraverso l'analisi della schematizzazione dei capi così come attuata dal legislatore europeo nel Regolamento.

Appare evidente *prima facie* il grande spazio riservato nel Capo IV alle figure del Titolare e del Responsabile del trattamento[71].

Non solo questo Capo, suddiviso a sua volta in ben cinque sezioni, è uno dei principali veicoli di introduzione di significative innovazioni della materia tra le quali i concetti della *privacy by design* e della *privacy by default*, gli strumenti della *Data protection impact assessment* e della *Prior consultation* e infine l'introduzione del *Data Protection Officer*. Grande importanza è riservata inoltre alla sezione riguardante la "*Sicurezza dei dati personali*" tra cui rientra l'istituto delle notificazioni susseguenti alla positiva verificazione di un'avvenuta *data breach* nei confronti del soggetto proprietario dei dati violati.

Immutata nella forma appare invece la parte inerente i "*Rights of Data Subject*", salvo l'introduzione all'interno del Capo III di due importantissime disposizioni che suggellano le conquiste giurisprudenziali degli ultimi anni, come il riconoscimento agli articoli 17 e 20 rispettivamente del c.d. diritto all'oblio[72] e del diritto alla portabilità dei dati.

A parte queste due significative innovazioni, non sembrano esserci particolari differenze tra Direttiva e Regolamento in questo specifico ambito di disciplina, al contrario di come accade invece per le norme inerenti gli obblighi, i diritti e i doveri, il regime di responsabilità e le modalità d'esecuzione che afferiscono alle

---

interamente o parzialmente automatizzato di dati personali e al trattamento non automatizzato di dati personali contenuti in un archivio o destinati a figurarvi.".

[71] Nella Direttiva 95/46/CE la terminologia delle due figure appare diversa: il Responsabile del trattamento (nel Reg. il "Titolare") è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali.* "; mentre l'Incaricato del trattamento (nel Reg. il "Responsabile") è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che elabora dati personali per conto del responsabile del trattamento*".

[72] Di cui una delle sentenze più famose a riguardo è senz'altro quella della Corte di Giustizia Europea nella causa C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protectiòn de Datos, Mario Costeja Gonzales*, 2014.

figure del *Controller* e del *Processor* (Titolare e Responsabile nella traduzione italiana).

È proprio da questi dettagli strutturali e di sistema che si intuisce il cambio di rotta per cui ha optato il legislatore europeo nella redazione del Regolamento e più in generale nell'ideazione della nuova tutela del diritto alla protezione dei dati personali.

Se nell'impianto della Direttiva Madre il rispetto delle disposizioni riguardanti i diritti dell'interessato era posta al centro della tutela giurisdizionale della protezione dei dati personali di un soggetto, ora appare evidente come il sistema di tutela si sia rovesciato principalmente a favore del rispetto delle norme sulle modalità trattamento del titolare e del responsabile del trattamento.

Dunque è forte la convinzione da parte del legislatore del 2016 che un'efficace protezione del diritto fondamentale alla protezione dati personali passi, ancor prima che dai diritti dell'interessato, necessariamente attraverso l'efficiente regolazione delle disposizioni inerenti il trattamento effettuato sui dati, ma soprattutto, tramite un'attenta puntualizzazione e un rigoroso coordinamento normativo delle regole che riguardano gli operatori del settore, la *best practice* alla quale quest'ultimi devono conformarsi nell'adempiere le proprie funzioni e infine, tramite il rispetto dei principi a garanzia della legittimità del trattamento e delle norme inerenti le misure di sicurezza adottabili.

Sarebbe riduttivo, e forse anche erroneo, affermare che i diritti della persona interessata perdono forza e importanza nella difesa degli interessi legati ai propri dati personali. Ma in un contesto normativo molto ampio e differenziato come quello dell'Unione e degli Stati che vi partecipano, in un panorama giuridico che si trova a dover rincorrere la velocità delle nuove tecnologie e del digitale, dove quantità difficilmente misurabili di dati viaggiano ad altissima frequenza lungo le direttrici spazio-temporali dettate dal *World Wide Web* (già il nome ci fa rendere conto di quanto i classici confini spaziali siano del tutto abbattuti quando si parla del mondo Internet), una tutela incentrata su istanze personali e/o collettive mirate a verificare il rispetto delle condizioni enunciate nei diritti che

disciplinano la materia, può comportare un onere forse troppo gravoso e un rallentamento nocivo nell'ottica di una tutela rapida ed efficace.

È indubbio che un accertamento di questo genere non può mancare del tutto, ma bisogna ricercare un mezzo più rapido, obiettivo e concreto che viene individuato dal Regolamento nella minuziosa disciplina di ciascuna fase del trattamento al quale i dati sono sottoposti.

Si tratta di un'intuizione di grandissima portata applicativa il cui intento è sicuramente rendere chiaro, predeterminato, conoscibile e il più "trasparente[73]" possibile il trattamento dei dati consentendo, allo stesso modo, una facile e agile rilevazione di anomalie e violazioni all'interno delle varie fasi del procedimento.

Di conseguenza la correttezza e la conformità di ogni singola fase del procedimento ai requisiti e ai principi predisposti dal Regolamento diventa non solo la prima e più importante garanzia a tutela degli interessi degli individui affinché i propri dati siano trattati e gestiti in modo conforme, ma inoltre si configura come presupposto fondamentale per un'efficace difesa e per il rispetto del diritto fondamentale alla protezione dati e di tutti quei diritti a quest'ultimo pertinenti.

Sicuramente questo rovesciamento di prospettiva, dotato di notevoli risvolti applicativi e che sembra essere in grado di confrontarsi abilmente con le sfide che pone l'odierna società digitalizzata, costituisce una novità.

Tuttavia bisognerà attendere gli esiti di una futura applicazione per verificare poi in concreto se la strategia ideata si rivelerà di successo.

---

[73] Il riferimento è chiaramente volto al richiamo del principio di Trasparenza che apre la Sezione I del Capo III (quello dedicato ai diritti dell'interessato) del Regolamento è che al par. 1 dell'art 12 prevede che "*Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato*." Dunque appare chiaro come gli obblighi del titolare e le modalità di svolgimento delle proprie funzioni siano strettamente inerenti alla soddisfazione della tutela dei diritti degli individui.

Sezione II

Le principali innovazioni introdotte dal Regolamento UE 2016/679

Le novità apportate alla materia dal Regolamento UE 2016/679, che mi sono limitato a citare brevemente nel paragrafo precedente, sono numerose e particolarmente innovative, improntate a dare un cambio di marcia e di modernità alla disciplina.

Allo stesso modo dove la normativa sembra riportare in maniera pressoché identica principi e concetti, di certo non sconosciuti nel settore, il legislatore europeo non manca di inventiva quantomeno nel rimodulare, ampliare e dettagliare, ove possibile, il tessuto normativo preesistente ispirato da istanze di completezza.

Tutto ciò si nota già nella prima parte del Regolamento quando al Capo I, al Capo II e al Capo III sono prese in esame rispettivamente le "*Disposizioni generali*", i "*Principi*" e i "*Diritti dell'interessato*".

1. Le Disposizioni generali

Per quanto riguarda "*Oggetto e finalità*" l'articolo 1 del Regolamento sembra riportare precisamente quanto stabilisce la Direttiva dove appunto conferma al paragrafo 2 che «*Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.* » e al successivo paragrafo 3 che «*La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.*».

In realtà il vero oggetto della disciplina deve rinvenirsi nel paragrafo 1 dell'articolo 1, che vuole specificare ancor di più, rispetto alla Direttiva, in quale direzione la disciplina sia rivolta affermando che « *Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al*

trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. ».

Ulteriori differenze si riscontrano inoltre, riguardo all'ambito d'applicazione tanto materiale quanto territoriale. Qui, preventivamente, bisogna ricordare che, essendo i due strumenti normativi a paragone diversi in quanto a struttura e finalità (la direttiva infatti è un mezzo d'armonizzazione normativa che richiede di conseguenza l'azione di implementazione necessaria degli Stati Membri; il regolamento essendo direttamente applicabile e avente efficacia diretta, al contrario entra "con forza propria" all'interno degli ordinamenti statali), l'opera di specificazione del legislatore europeo è decisamente più marcata nel definire l'ambito d'applicazione della nuova normativa.

L'ambito d'applicazione *materiale* rimane pressoché invariato rispetto alla disposizione della Direttiva 95/46. Infatti la normativa continua ad applicarsi a tutti quei trattamenti interamente o parzialmente automatizzati di dati personali, compreso il trattamento non automatizzato di dati personali contenuti in archivio o destinati a figurarvi. Allo stesso modo sono riportate le cause di esclusione del trattamento dei dati e cioè: quando i trattamenti esulano dal campo d'applicazione del diritto UE; quando si tratta di un'attività effettuata dagli Stati membri rientrante nell'ambito di applicazione del Titolo V, capo II, TUE (Disposizioni Specifiche sulla Politica Estera e di Sicurezza Comune); quando si tratta di un'attività effettuata dalle autorità competenti nell'ambito del diritto penale (prevenzione, indagine, accertamento o perseguimento o esecuzione di sanzioni penali), incluse la salvaguardia contro minacce alla pubblica sicurezza e la prevenzione delle stesse; e infine, quando riguarda trattamenti effettuati da persone fisiche in attività aventi carattere puramente personali o domestiche[74].

[74] A tal proposito un certo grado di innovazione si percepisce dall'analisi del Considerando n.18 che include (ormai inevitabilmente data l'onnipresenza di tali tecnologie all'interno della vita quotidiana di ognuno di noi) nelle attività di tipo domestico anche l'utilizzo dei *social networks*. Allo stesso modo viene precisato che in ogni caso: «*il presente regolamento si applica ai titolari del trattamento o ai responsabili del trattamento che forniscono i mezzi per trattare dati personali nell'ambito di tali attività a carattere personale o domestico.*».

Al contrario l'ambito d'applicazione *territoriale* è quello che risulta decisamente innovato rispetto a quanto previsto dalla Direttiva del '95.

In questo senso il Regolamento è stato ampiamente recettivo di tutti quegli orientamenti giurisprudenziali[75] e dei pareri espressi dal Gruppo art.29[76], che in quest'ambito hanno sempre spinto per una più ampia e flessibile interpretazione della nozione di stabilimento.

Il Regolamento in questo caso sembra dover adempiere un compito più ampio rispetto a quello della Direttiva: quest'ultima infatti doveva individuare di volta in volta quale fosse il diritto nazionale applicabile secondo "*il criterio dello stabilimento*" tanto all'interno quanto all'esterno dell'Unione; mentre al contrario il Regolamento, predisponendo una disciplina uniforme in tutto il territorio europeo, deve constatare se risulta essere applicabile o meno la normativa europea in tema di protezione dei dati personali e, nel caso, decidere quale tra le diverse Autorità Garanti sul territorio debbano operare o possano intervenire in supporto[77].

Il criterio dello stabilimento rimane sempre centrale all'interno della disposizione anche se chiaramente allarga il suo spettro visivo in quanto l'articolo 3 stabilisce che il Regolamento «*si applica al trattamento di 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.* ».

---

[75] Nella sentenza *Google Spain SL* i giudici europei osservano che per determinare l'esistenza di uno stabilimento in uno Stato Membro diverso "*occorre valutare sia il grado di stabilità dell'organizzazione sia l'esercizio effettivo delle attività in tale altro Stato membro, prendendo in considerazione la natura specifica delle attività economiche e delle prestazioni dei servizi in questione*", guardando dunque a una nozione sostanziale di stabilimento e non prettamente formale. Vedi causa C-131/12, *Google Spain SL, Google Inc.* c. *Agencia Española de Protectiòn de Datos, Mario Costeja Gonzales*, 2014. Inoltre la Corte fonda l'applicabilità della Direttiva sul fatto che Google Spain costituisce una filiale di Google Inc. nel territorio spagnolo, volta alla comunicazione e alla vendita di comunicazioni commerciali dirette ai residenti dello Stato membro e pertanto integri uno "stabilimento" ai sensi dell'art. 4. Sul punto, G. CAGGIANO, *Attività di stabilimento e trattamento dei dati personali,* in *Dir.inf.*, 2014.

[76] A tal proposito si consultino rispettivamente il Parere 1/2008 (WP 148) "*sugli aspetti della protezione dei dati connessi ai motori di ricerca*" e il Parere 8/2010 (WP 179) "*sul diritto applicabile*" entrambi consultabili sul sito www.ec.europa.eu

[77] A tal proposito il nuovo Regolamento dedica molta attenzione all'aspetto della cooperazione dedicando l'intero Capo VII alla "*Cooperazione e Coerenza*" e istituendo allo stesso tempo la figura dell'Autorità di Controllo Capofila (*Lead supervisory authority*) previsto all'articolo 56 Reg.

Quello previsto al par.1 dell'articolo 3 si configura come il criterio generale applicabile, per cui le disposizioni del Regolamento si applicano in relazione alle attività da parte del titolare o responsabile del trattamento di uno stabilimento che svolge la sua attività all'interno del territorio dell'Unione, indipendentemente dal fatto che il trattamento avvenga interamente o anche solo parzialmente all'interno dell'Unione Europea.

Ai successivi paragrafi sono previste delle particolari ipotesi per cui la normativa regolamentare è comunque applicata, nonostante il trattamento dei dati avvenga all'esterno del territorio dell'Unione e sia effettuato da agenti (titolare e responsabile) che comunque non sono stabiliti all'interno dell'Unione Europea. Ciò è consentito in base a un collegamento territoriale che si instaura tra operatori e trattamento dei dati degli interessati che si trovano nell'Unione, da una parte, e quelle attività che esplicano effetti direttamente nel territorio dell'Unione, dall'altra.

Così facendo, il Regolamento sarà applicabile anche quando le attività di trattamento dei dati personali di interessati situati nell'Unione, anche se effettuate da titolari o responsabili del trattamento che non sono stabiliti nel territorio UE, riguardano rispettivamente:

a) l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato;
b) il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione; e infine
c) qualora il trattamento sia effettuato in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico.

Emerge perciò con forza la volontà del diritto dell'Unione di porsi come modello forte di tutela della Privacy, teso a garantire al cittadino europeo un medesimo livello di protezione a prescindere dal luogo in cui materialmente si svolge il trattamento dei propri dati personali, specialmente dinanzi alle molteplici

possibilità offerte dalle nuove tecnologie di svuotare di contenuto e rendere inoperante il diritto alla protezione dei dati personali[78].

Un'altra sostanziale differenza tra Regolamento e Direttiva si rileva all'articolo 4 rubricato "*Definizioni*". Più volte si è sottolineata la quasi "maniacale" attenzione al dettaglio applicata dal legislatore del 2016 che qui sembra operare con tutta la sua forza. Basti pensare che la stessa identica disposizione nella Direttiva 95/46 è composta solamente da otto definizioni comprendenti quelle di : dato personale, trattamento di dati personali, archivio di dati personali, responsabile del trattamento (ora titolare), incaricato del trattamento (ora responsabile), terzi, destinatario e consenso della persona interessata.

Al contrario il Regolamento annovera ben ventisei definizioni di cui alcune di esse composte da più sottolettere e comunque le definizioni già presenti nella Direttiva sono state sottoposte immancabilmente ad un'opera di "restauro".

A tale proposito si prenda in considerazione la definizione di *dato personale*.

Esso nella struttura della definizione rimane identico a quanto previsto dalla Direttiva Madre, per cui un dato di carattere personale consiste sempre in una qualsiasi informazione riguardante una persona fisica identificata o identificabile (il c.d. interessato); però, nel determinare quando una persona sia reputata "identificabile", ecco che l'opera di ammodernamento si coglie in maniera esplicita.

Ciò è ricavabile in particolare dall'ampliamento della categoria dei c.d. identificativi che, oltre alle tipologie classiche come il nome, il numero di identificazione e gli elementi caratteristici dell'identità fisica, fisiologica, psichica, economica, culturale e sociale, richiamano esplicitamente tipologie di identificativi strettamente collegati alle tecnologie sviluppatesi negli ultimi anni: come i dati relativi all'ubicazione (si pensi ai dati trasmessi dai dispositivi GPS), identificativi generici online, ovvero elementi caratteristici dell'identità genetica di una persona.

[78] M.G. STANZIONE, *Genesi ed Ambito di Applicazione,* Cap II, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 31.

Infatti nel sistema delle definizioni il Regolamento, per la prima volta in assoluto, introduce due categorie di dati afferenti alla sfera biologica e genetica della persona: categorie di dati che, in determinati settori (ad esempio quello medico) e mediante l'utilizzo di determinate tecnologie (come quelle che permettono scanner biometrici facciali o rilevazioni fotografiche particolarmente invadenti), sono particolarmente suscettibili di non poco rilevanti violazioni in tema di privacy, di protezione dei dati personali e forse più in generale di libertà di autodeterminazione.

Di conseguenza sono inserite nel novero delle definizioni tre importanti categorie di dati: i **dati genetici** definiti come «*i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione.*»; i **dati biometrici** descritti come «*i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici*.» nonché infine i **dati relativi alla salute** considerati come quei «*dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute*».

Anche la definizione di *trattamento*, seppur non in maniera radicale, subisce delle variazioni in quanto alle classiche operazioni che ritroviamo anche nella Direttiva Madre, come ad esempio la raccolta, l'organizzazione, la conservazione, la modifica, l'estrazione, la consultazione, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la cancellazione o distruzione, sono aggiunte nuove operazioni quali la strutturazione, l'adattamento, l'uso e infine la limitazione, la cui definizione viene espressa al successivo numero e che, nello

specifico, consiste in un «*contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro*».

Allo stesso modo le definizioni degli agenti principali delle operazioni di trattamento non variano sostanzialmente dalle definizioni previste dalla Direttiva 95/46 se non esclusivamente a livello strettamente nominale. Infatti il soggetto ora definito come "Titolare", nella Direttiva assumeva il nominativo di Responsabile del trattamento e il soggetto che adesso è chiamato "Responsabile", nella normativa del '95 era denominato Incaricato del trattamento.

Risulta inoltre ampliata la definizione di *consenso dell'interessato*. Appare chiara qui la volontà del legislatore del 2016 di voler rendere il più puntuale possibile i requisiti del consenso, affinché quest'ultimo possa considerarsi validamente prestato, e onde evitare, altresì, pericolose derive interpretative suggeribili dalla generalità testuale. Il legislatore a livello semantico infatti, risulta chiaro e risoluto e, se nella definizione derivante dalla Direttiva del '95 il consenso si presentava come «*qualsiasi manifestazione di volontà libera, specifica e informata con la quale la persona interessata accetta che i dati personali che la riguardano siano oggetto di un trattamento*», il "nuovo" consenso si presenta ora pur sempre come una manifestazione di volontà libera, specifica e informata, ma deve essere inoltre *inequivocabile*. Non solo, al fine di evitare che il consenso possa essere interpretato come presunto, l'interessato manifesta il proprio assenso, affinché i dati che lo riguardano possano essere oggetto di trattamento, «*mediante dichiarazione o azione positiva inequivocabile*».

A parte poi, l'inserimento di ulteriori definizioni utili al fine di comprendere meglio il campo d'azione e i vari operatori del settore della protezione dei dati personali come ad esempio le definizioni di violazione dei dati personali[79], di norme vincolanti di impresa[80], oppure di stabilimento principale e di gruppo

[79] Per *Violazione dei dati personali* si intende 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.

[80] Le *Norme vincolanti di impresa* (in inglese le *binding corporate rules*) sono quelle politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati

imprenditoriale, di autorità di controllo e di autorità di controllo interessata, di trattamento transfrontaliero, davvero innovativa risulta l'introduzione di due definizioni importantissime: quelle di **profilazione** e **pseudonimizzazione**.

La Profilazione è intesa come «*qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica*».

Invece, per Pseudonimizzazione si intende quel «*trattamento dei dati personali in modo tale che i dati personali 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*».

Profilazione e Pseudonimizzazione sono due *topics* fondamentali di cui mi riserbo però una più completa trattazione nei paragrafi successivi, data l'importanza nel panorama del diritto alla protezione dei dati personali e del ruolo centrale che assumono nella nuova regolamentazione. Si può intanto anticipare che le due procedure se non appositamente gestite e controllate possono comportare serissimi problemi per la protezione dei dati personali delle persone.

La profilazione infatti consiste in una particolare modalità di trattamento e raccolta di grandissime quantità di informazioni riguardanti i comportamenti degli utenti nel web, utilizzata per lo più a scopi commerciali e pubblicitari da grandi imprese che operano nel mercato digitale. Ciò permette alle grandi imprese commerciali di creare dei veri e propri "profili digitali" dei vari utenti,

---

personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune.

suddividendoli in categorie, in modo tale da differenziare la clientela e di conseguenza fornire servizi più mirati a seconda dei risultati derivanti dalle operazioni di analisi dei dati ricavati. Se da un lato un servizio di questo genere comporta sicuramente un'offerta più pertinente rispetto alla domanda e in generale una migliore accuratezza dei servizi e prodotti proposti, è comunque fondato il timore che uno sconsiderato, indiscriminato e generalizzato utilizzo della tecnica di profilazione possa portare ad un controllo globale e costante dei comportamenti della popolazione, andando ad incidere negativamente su aspetti della vita privata delle persone particolarmente sensibili come il rendimento professionale, la situazione economica, l'ubicazione e le preferenze personali.

La pseudonimizzazione si potrebbe dire impropriamente consistere in una "procedura alternativa per il riutilizzo" di quei dati che secondo il principio di finalità non sono più corrispondenti ai requisiti per i quali furono raccolti e trattati e in quanto tali andrebbero cancellati.

Infatti il principio generale è che i dati andrebbero conservati in modo da consentire l'identificazione delle persone interessate per un arco di tempo non superiore a quello necessario al conseguimento delle finalità per cui sono stati raccolti o diversamente cancellati[81]. L'ulteriore utilizzo di tali dati può essere consentito per altre finalità a patto che i suddetti dati siano anonimizzati o pseudonimizzati. Se l'anonimizzazione consiste in quella procedura che consente l'uso solamente dopo che tutti gli elementi identificativi siano stati eliminati[82], la pseudonimizzazione è quel processo volto a "camuffare" alcuni identificatori che riconducono all'identità del soggetto senza però eliminarli del tutto. Si tratta di una tecnica che è molto utilizzata specialmente nell'ambito della ricerca scientifica, statistica e medica. Fondamentale è che i dati così trasformati non

[81] Si vedano articolo 6, par.1, lett. e), Direttiva 95/46/CE e articolo 5, lett. e), Convenzione n. 108/1981.
[82] Sul tema si vedano il Parere n. 3/97, su *"Anonymity on Internet"* (WP29 n. 6) e il recente Parere n. 5/2014 del Gruppo art. 29 , riguardo "*Tecniche di anonimizzazione*", 10 aprile 2014 (WP29 n.216).

mantengano elementi identificativi tali che, con un *ragionevole sforzo*[83], possano ricondurre all'identità della persona anonimizzata o pseudonimizzata.

Va però precisato che i dati anonimizzati non sono più ritenuti dati avente carattere personale e in quanto tali non sono più soggetti alle norme inerenti la protezione dei dati personali, mentre al contrario i dati pseudonimizzati sono ritenuti informazioni su persone identificabili *indirettamente* e così facendo sottoposti al regime di disciplina del Regolamento.

2. I Principi nel nuovo Regolamento

Come affermato nel paragrafo precedente, profili interessanti sono riportati e introdotti anche nei Capi II e III, rispettivamente in tema di "*Principi*" e "*Diritti dell'interessato*".

Quasi a voler rimarcare ancor di più la centralità che assume il Trattamento nella nuova disciplina, il Regolamento del 2016 in apertura del Capo relativo ai Principi non intitola più il primo articolo "Principi relativi alla Qualità dei Dati"(art. 6 Dir. 95/46), ma decide di rinominarlo "Principi applicabili al trattamento di dati personali". Ispirato poi alla massima chiarezza possibile suddivide in sei lettere i principi fondamentali relativi al trattamento e alle qualità che i dati devono possedere inserendo alla fine del periodo, tra parentesi e in modo chiaro, il principio generale sotteso.

[83] Qui il considerando n. 26 del Regolamento 2016/679 riprende determinazioni già affrontate nella Direttiva del '95 e dall'operato del Gruppo di Lavoro comune ex. Art. 29 in tema di anonimizzazione, pseudonimizzazione e nel determinare in cosa consiste il ragionevole sforzo che qui riporto integralmente: « *È auspicabile applicare i principi di protezione dei dati a tutte le informazioni relative a una persona fisica identificata o identificabile. I dati personali sottoposti a pseudonimizzazione, i quali potrebbero essere attribuiti a una persona fisica mediante l'utilizzo di ulteriori informazioni, dovrebbero essere considerati informazioni su una persona fisica identificabile. Per stabilire l'identificabilità di una persona è opportuno considerare tutti i mezzi, come l'individuazione, di cui il titolare del trattamento o un terzo può ragionevolmente avvalersi per identificare detta persona fisica direttamente o indirettamente. Per accertare la ragionevole probabilità di utilizzo dei mezzi per identificare la persona fisica, si dovrebbe prendere in considerazione l'insieme dei fattori obiettivi, tra cui i costi e il tempo necessario per l'identificazione, tenendo conto sia delle tecnologie disponibili al momento del trattamento, sia degli sviluppi tecnologici. I principi di protezione dei dati non dovrebbero pertanto applicarsi a informazioni anonime, vale a dire informazioni che non si riferiscono a una persona fisica identificata o identificabile o a dati personali resi sufficientemente anonimi da impedire o da non consentire più l'identificazione dell'interessato.*».

Ecco allora che il lettore del testo normativo rapidamente può comprendere i principi ai quali tanto i dati, quanto il trattamento alla quale i dati sono sottoposti, devono sottostare:

a) *liceità, correttezza e trasparenza*, se trattati in modo lecito, corretto e trasparente;
b) *limitazione della finalità*, se raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo tale che con suddette finalità non siano incompatibili;
c) *minimizzazione dei dati*, se adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;
d) *esattezza*, se esatti e dove necessario aggiornati e se sono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente le inesattezze dei dati rispetto alle finalità;
e) *limitazione della conservazione*, se i dati sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per cui sono trattati;
f) *integrità e riservatezza*[84], se trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti illeciti o non autorizzati e dalla perdita, dalla distruzione o dal danno accidentale;
g) *responsabilizzazione*, dove è previsto che il titolare del trattamento è il soggetto deputato al rispetto di tutti questi principi e che in capo a quest'ultimo sorge l'obbligo di comprovarne il rispetto.

All'articolo 6 del nuovo Regolamento invece sono raggruppati i requisiti affinché un trattamento possa ritenersi lecito e cioè quando ricorrano almeno una delle seguenti condizioni:

[84] Lettera inserita con Regolamento UE/2016/679, in quanto non presente come principio nella precedente Direttiva 95/46/CE. Si intende ancora più chiaramente l'importanza riservata nel Regolamento ai principi e alle modalità riferite ad un corretto trattamento dei dati come principale strumento per la tutela del diritto alla protezione dei dati personali che passa principalmente dalle "misure di sicurezza" apprestate al procedimento.

a) l'interessato abbia espresso il proprio consenso al trattamento dei dati per una o più specifiche finalità;
b) il trattamento sia necessario all'esecuzione di un contratto in cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dell'interessato stesso;
c) il trattamento è necessario per adempiere ad un obbligo legale del titolare del trattamento;
d) il trattamento è necessario per la salvaguardia di interessi vitali dell'interessato o di un'altra persona fisica;
e) il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento;
f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi, i diritti e le libertà fondamentali dell'interessato in particolare se quest'ultimo è un minore.

Uno dei profili più interessanti inseriti in questo capo è senza dubbio la considerazione che il legislatore europeo pone riguardo la condizione del minore. Infatti nella società moderna i minori inevitabilmente, fin da giovanissimi, arrivano a diretto contatto con le nuove tecnologie come il web, le applicazioni di ogni genere scaricabili sugli smartphone, con le piattaforme social senza essere consapevoli di come, in cambio dell'utilizzo di questi servizi, i propri dati vengano poi utilizzati (ma chi infondo è pienamente consapevole?).

Lodevole, dunque in questa prospettiva, l'inserimento da parte del legislatore del 2016 di due esplicite previsioni inerenti il consenso:

all'articolo 7 le "Condizioni per il consenso" in generale e all'articolo 8 le "Condizioni applicabili al consenso del minore in relazione ai servizi della società dell'informazione".

L'articolo 7 prevede come obbligo in capo al titolare che, qualora il trattamento sia basato sul consenso, egli deve essere in grado di dimostrare che l'interessato

abbia prestato il proprio consenso, determinando qui quello che potremmo chiamare/definire un'inversione dell'onere probatorio riguardo il rilascio di un consenso valido al trattamento dei dati personali. È inoltre previsto che l'interessato abbia in qualsiasi momento il diritto di revocare il proprio consenso liberamente, e con la facilità con la quale lo ha prestato, specificando comunque che la revoca del consenso non pregiudica il trattamento avvenuto precedentemente e in maniera conforme al consenso anteriormente prestato. Infine è prevista, quale ultima condizione per valutare se il consenso sia stato liberamente prestato, che si tenga conto *nella massima considerazione* delle ipotesi in cui l'esecuzione di un contratto o la prestazione di un servizio sia subordinata alla prestazione del consenso, da parte dell'interessato, ad un trattamento di dati personali non necessario ai fini dell'esecuzione del contratto o alla prestazione del servizio stesso. In questo caso il consenso prestato dall'interessato all'ulteriore trattamento non può dirsi realmente libero, poiché chiaramente condizionato dalla necessità da parte dell'utente di usufruire del servizio, che altrimenti gli verrebbe negato.

L'articolo 8 invece pone come condizioni necessarie per la validità del consenso prestato da un minore, ai fini della liceità del trattamento, che quest'ultimo abbia almeno compiuto il 16esimo anno di età e in caso contrario, ove il minore abbia un età inferiore ai 16 anni, che il consenso sia prestato e/o autorizzato dal titolare della potestà genitoriale.

Per quanto riguarda invece la categoria dei *Dati sensibili* anche quest'ultima subisce delle parziali modifiche e un ampliamento di sistema derivante dall'introduzione delle nuove categorie di dati inseriti, come visto nelle Definizioni all'articolo 4 Reg., e dall'inserimento di ulteriori cause in deroga al generale divieto di trattamento dei dati personali c.d. sensibili previste al paragrafo 2 dell'articolo 9.

Infatti l'articolo 9 al par. 1, sancisce il divieto generale di trattamento di tutti quei dati personali capaci di rivelare: l'origine razziale o etnica, le opinioni politiche o l'appartenenza sindacale, le convinzioni religiosi o filosofiche, nonché il

trattamento di dati genetici o biometrici intesi a identificare una persona in modo univoco e infine i dati relativi alla salute, alla vita sessuale o all'orientamento sessuale della persona.

Il par. 2 invece, come detto, prevede delle deroghe per cui il divieto generale al trattamento dei dati sensibili di una persona non opera.

Si tratta di particolari situazioni per le quali il trattamento dei dati risulta inevitabile o più in generale legittimo[85], per esempio quando:

a) l'interessato abbia prestato il proprio consenso esplicito al trattamento dei dati per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o di uno Stato membro preveda che l'interessato non possa revocare il consenso successivamente;
b) il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto al lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o di uno Stato membro o da un contratto collettivo nazionale e in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato;
c) il trattamento sia necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato non sia nella capacità fisica o giuridica di prestare il proprio consenso;
d) il trattamento sia effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri,

[85] Si ricorda infatti che il diritto fondamentale alla protezione dei dati personali, con tutte le sue componenti più o meno delicate e importantissime rispetto alla tutela della libertà delle persone, non è un diritto assoluto e di conseguenza è soggetto di volta in volta al bilanciamento con altri diritti e libertà per cui in particolari casi "cede" di fronte a interessi ritenuti prevalenti. Si veda a tal proposito F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016, che dedica alla tematica l'intero capitolo secondo intitolato appunto "*Il bilanciamento dei diritti nel quadro europeo della protezione dati*" dove analizza esaurientemente le dinamiche del bilanciamento tra la protezione dei dati personali con vari diritti e libertà come: i diritti di libertà d'espressione e manifestazioni artistica o di stampa, il diritto d'accesso alle informazioni o della proprietà privata ecc...

gli ex membri, soggetti che hanno regolari contatti con la fondazione e che i dati non siano trasmessi all'esterno senza il consenso dell'interessato;

e) il trattamento riguardi dati resi manifestamente pubblici dall'interessato;
f) il trattamento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria od ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni;
g) il trattamento sia necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o di uno Stato membro, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
h) il trattamento sia necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali;
i) il trattamento sia necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici;
j) il trattamento sia necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89[86], paragrafo 1, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.

[86] L'articolo 89 del Reg. intitolato "Garanzie e deroghe relative al trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici" al paragrafo 1 prevede che «*Il trattamento a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici è soggetto a garanzie adeguate per i diritti e le libertà dell'interessato, in conformità del presente regolamento. Tali garanzie assicurano che siano state predisposte misure tecniche e organizzative, in particolare al fine di garantire il rispetto del principio della minimizzazione dei dati. Tali misure possono includere la pseudonimizzazione, purché le finalità in questione possano essere conseguite in tal modo. Qualora possano essere conseguite attraverso il trattamento ulteriore che non consenta o non consenta più di identificare l'interessato, tali finalità devono essere conseguite in tal modo.* »

3. I Diritti dell'interessato

Nella Direttiva 95/46/CE il catalogo contenente i diritti dell'interessato era spalmato su più sezioni all'interno del Capo II inerente le "Condizioni Generali di Liceità dei Trattamenti di Dati Personali".

Il legislatore europeo del 2016 al contrario decide di dedicare un intero Capo, suddiviso in ben cinque sezioni[87], ai diritti facenti capo all'interessato in modo da catalogarli in maniera ordinata e sistematica. L'obiettivo è senza dubbio quello di estrapolare dalla massa aggrovigliata delle condizioni di liceità del trattamento, la parte relativa ai diritti costruendo un sistema più chiaro, omogeneo, autonomo e coordinato, in modo tale da renderne senz'altro più agile la lettura e con lo scopo inoltre di far risaltare le innovazioni apportate in quest'ambito di disciplina.

Il Capo III infatti presenta rilevanti novità per il diritto alla protezione dei dati personali come il Principio di Trasparenza, tanto per quanto riguarda il trattamento (come visto ex art.6 Reg.) quanto per le comunicazioni e l'informativa, ovvero per l'introduzione di nuovi diritti come il Diritto alla Rettifica, il Diritto alla Cancellazione (il c.d. diritto all'oblio), il Diritto di Limitazione di trattamento e infine il Diritto alla Portabilità dei dati.

Per quanto riguarda il principio di trasparenza il Regolamento lo introduce in pianta stabile, in primo luogo, nell'apparato dei principi applicabili al trattamento dei dati personali dove insieme ai canonici principi di liceità e correttezza, come abbiamo visto, l'articolo 5 stabilisce che i dati personali siano trattati in modo lecito, corretto e *trasparente* nei confronti dell'interessato; in secondo luogo inserendolo in apertura del capo relativo i diritti dell'interessato, determinando le modalità attraverso le quali il principio si estrinseca in concreto, specialmente per

[87] Il Capo III intitolato "*Diritti dell'Interessato*" si suddivide nelle seguenti sezioni:
a) Sezione I: Trasparenza e modalità;
b) Sezione II: Informazione e accesso ai dati personali;
c) Sezione III: Rettifica e cancellazione;
d) Sezione IV: Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche;
e) Sezione V: Limitazioni.

quanto riguarda l'informativa e le comunicazioni all'interessato, e definendolo come un presupposto giuridico fondamentale per un efficace esercizio dei diritti appartenenti alla persona.

È indubbio, infatti, che il principio di trasparenza sia strettamente connesso in profondità con le trame di altri istituti come quello dell'informazione, delle comunicazioni destinate all'interessato, ma non solo più in generale la trasparenza è strettamente collegata all'operatività dei diritti facenti capo al soggetto *in primis* il diritto d'accesso. Immaginiamo uno schema a struttura triangolare ai cui vertici troviamo rispettivamente Trasparenza, Informazione ed Esercizio dei Diritti: senza trasparenza non vi è informazione (o quantomeno è difficile ottenere un quadro completo, chiaro e perché no veritiero), se non vi è informazione non può seguire un efficiente esercizio dei diritti da parte dei soggetti interessati. Al fine di chiudere lo schema, e renderlo completo, è necessaria la compresenza di tutti e tre gli elementi, essendo infatti l'uno il presupposto dell'altro.

L'articolo 12 a tal proposito prevede un vero e proprio obbligo in capo al titolare del trattamento che deve adottare tutte le misure appropriate per fornire a chi è legittimato a farne richiesta, le informazioni di cui agli artt. 13 e 14 (qualora i dati personali rispettivamente non siano stati ottenuti presso l'interessato, oppure siano stati raccolti presso l'interessato), ovvero le comunicazioni di cui agli artt. dal 15 al 22 (cioè tutto l'insieme di diritti e obblighi che partono dal diritto d'accesso e terminano con la disposizione relativa al processo decisionale automatizzato relativo alle persone fisiche, compresa la profilazione) e all'art. 34 (che prevede le comunicazioni in caso di violazione dei dati personali dell'interessato). Fondamentale è che tali informazioni e comunicazioni avvengano in «*forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori.*».

Come anche enunciato espressamente al 39esimo Considerando l'applicazione del principio di trasparenza deve essere, nello specifico, mirata a rendere il più

chiaro e comprensibile possibile per l'interessato quelle che sono « *le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che li riguardano nonché la misura in cui i dati personali sono o saranno trattati* »; non solo, necessario al fine di assicurare e garantire la correttezza del trattamento è fondamentale che sia data un'informativa chiara e precisa riguardante «*l'identità del titolare del trattamento e le finalità del trattamento e ulteriori informazioni per assicurare (...) alle persone fisiche interessate e ai loro diritti, di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano*»; inoltre in un'ottica di maggiore completezza del patrimonio informativo dell'interessato riguardo il trattamento al quale sono sottoposti i dati che lo riguardano si asserisce che «*le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali*» e che sia «*utilizzato un linguaggio semplice e chiaro*».

La trasparenza dei dati e delle modalità con cui avviene il trattamento è dunque funzionale alla possibilità per l'interessato di seguire i propri dati, di autorizzarne modifiche, richiedere aggiornamenti e fare in modo di vietare e richiedere l'intervento per evitare abusi.

Se la trasposizione dei diritti e dell'identità di una persona avviene dal tradizionale piano fisico dell'*habeas corpus*, su di un altro completamente nuovo come quello digitale, trasformandosi in un vero e proprio *habeas data*, è allora doveroso che vi sia un'adeguata tutela rafforzata tanto del corpo quanto della mente elettronica, con garanzie e responsabilità che il principio di trasparenza introduce nel nuovo Regolamento dettando chiari precetti ai titolari del trattamento, alle imprese e alle amministrazioni affinché adottino politiche concise, trasparenti, chiare e facilmente accessibili mediante informazioni rese con linguaggio semplice e chiaro[88].

[88] G. DI GENIO,*Trasparenza e Accesso ai dati personali,* Cap VIII, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 164.

Al fine di una tutela rafforzata sono previsti ulteriori obblighi in capo al titolare del trattamento come quando al par. 2 si specifica che il titolare agevola l'esercizio dei diritti dell'interessato e che non può rifiutarsi di soddisfare la richiesta dell'interessato al fine di esercitare tali diritti, o ancora quando al par. 3 è fatto obbligo al titolare di fornire le informazioni relative all'azione intrapresa senza ingiustificato ritardo nel termine massimo di un mese, prorogabile di due mesi, previa comunicazione all'interessato dei motivi di ritardo.

Però, così delineato, il principio di trasparenza sembra operare esclusivamente *ex post*, e cioè in un momento successivo al trattamento, che si presuppone in questo caso già avvenuto, come un requisito da rispettare affinché il complesso delle comunicazioni e delle informazioni richieste dall'interessato siano *compliant* rispetto al dettato normativo che richiede la massima comprensione e la chiara conoscibilità da parte delle persone alle quali i dati appartengono.

Invero, il principio di trasparenza deve porsi già in un momento antecedente rispetto al complesso di operazioni alle quali i dati verranno successivamente sottoposti, e cioè ancor prima che il titolare del trattamento arrivi in possesso dei dati dell'utente, in una fase in cui trasparenza e consenso dell'interessato sono strettamente correlati.

Infatti affinché il principio di trasparenza possa dirsi completato, nell'ottica di favorire con la chiarezza massima la consapevolezza dell'interessato, in merito all'utilizzo che verrà fatto dei propri dati personali, deve necessariamente porsi prima della richiesta di acquisizione dei dati personali da parte del titolare, nella fase appunto del rilascio del consenso.

La persona alla quale appartengono i dati deve potersi prefigurare già prima di una valida prestazione del consenso (e in realtà tali informazioni a monte sono funzionali proprio affinché l'interessato presti liberamente e consapevolmente il proprio consenso) quale sarà l'utilizzo che verrà fatto dei propri dati, a quali operazioni di trattamento saranno sottoposti gli stessi, per quanto tempo, con quali modalità e quali sono le specifiche finalità per le quali sono trattati. Soltanto in questo modo può dirsi realmente consapevole e pienamente informata

la persona interessata in merito al trasferimento e all'utilizzo dei propri dati personali al quale ha acconsentito, solo in questo modo può dirsi pienamente rispettato quel diritto all'autodeterminazione informativa che è la sostanza del diritto alla protezione dei dati personali, quantomeno sotto il profilo della disponibilità, della libera gestione e della autonoma spendibilità del patrimonio informativo che appartiene ad ognuno di noi.

Inoltre il principio di trasparenza è indissolubilmente legato al diritto d'accesso dell'interessato che, nell'ottica della tutela del diritto alla protezione dei dati personali, riveste un'importanza strategica rilevante nella dinamica procedurale, in quanto è funzionale, potremmo dire anche prodromico rispetto all'esercizio delle altre tipologie di diritti connessi come quello di rettifica, limitazione, opposizione, oblio e portabilità dei dati.

Non di rado accade che l'utente accetti di rilasciare un consenso anticipato e generale, sopraffatto dalla forza economica schiacciante, che nella dialettica della domanda e offerta di servizi sul mercato digitale, hanno banche, multinazionali e aziende-colosso del settore (si pensi ai social network), e che è posto come condizione indispensabile alla possibilità di usufruire del servizio. Nella maggior parte dei casi infatti le istanze garantiste nei confronti del nostro patrimonio dati sono rapidamente sostituite dai benefici e dai comfort che ricaviamo da tale sottoscrizione, come fosse una "firma di un patto col diavolo".

Ora lungi da me, in uno scompenso distopico, voler paragonare le multinazionali del settore e le Over The Top a Satana in persona, e voler affermare in modo presuntuoso che i servizi e le tecnologie proposte da queste aziende sono meri specchi per le allodole che hanno in realtà, come secondo fine, quello di soggiogare la nostra "anima digitale", ma non mi allontano troppo dalla realtà nell'affermare che oggigiorno la consapevolezza dei nostri dati e dei danni che possono derivare da un uso illegittimo, lascia il posto alla prospettiva di una vita più facile grazie alle comodità offerte dalle nuove tecnologie e dai servizi, a quest'ultime, connessi.

È in quest'ottica che trasparenza e diritto d'accesso assumono un'importanza significativa nella nuova disciplina: trasparenza come regola metodologica da attuare nella fase pre-trattamento (come una delle condizioni di validità del consenso) e nella fase post-trattamento (per quanto riguarda comunicazioni e informativa inerente le operazioni effettuate sui dati ecc..); e diritto d'accesso come verifica posta in essere dall'interessato al fine di sondare il rispetto dei principi sottesi ad un corretto trattamento dei proprio dati e di avere, inoltre piena contezza dei propri dati personali in un preciso momento[89].

La categoria dell'accesso si presenta come struttura unificante, che rende concreto l'esercizio dei poteri attribuiti alla persona in una molteplicità di situazioni dall'entrata nella rete al rapporto con le diverse categorie di beni comuni, al permanente controllo del sé elettronico[90] e come detto in precedenza apre la porta, quale presupposto procedurale, alla possibilità di esperimento degli altri diritti dell'interessato.

L'articolo 15 prevede dunque che l'interessato abbia il diritto di ottenere da parte del titolare la conferma in merito all'esistenza o meno di un trattamento di dati che lo riguardano e in tal caso ottenere l'accesso a tali dati nonché essere informato in merito:

a) alle finalità del trattamento;
b) alle categorie di dati personali sottoposte a trattamento;
c) ai destinatari a cui i dati personali saranno comunicati e se quest'ultimi appartengono a paesi extra UE o a organizzazioni internazionali;
d) al periodo di conservazione previsto per i dati e, quando non è possibile definirlo, quantomeno richiedere quali siano i criteri utilizzati per determinare tale periodo;

[89] Come anche esplicitato nel considerando n. 63 del Reg. quando si afferma che «*Un interessato dovrebbe avere il diritto di accedere ai dati personali raccolti che la riguardano e di esercitare tale diritto facilmente e a intervalli ragionevoli, per essere consapevole del trattamento e verificarne la liceità.*»

[90] *Ivi*, p.170.

e) all’esistenza da parte dell’interessato del diritto di chiedere direttamente al titolare la rettifica, la cancellazione dei dati, oppure il diritto di richiedere la limitazione o di opporsi al trattamento;
f) al diritto di proporre reclamo a un’autorità di controllo;
g) all’origine dei dati, qualora quest’ultimi non siano stati raccolti direttamente presso l’interessato;
h) all’esistenza di un processo decisionale automatizzato, compresa la profilazione, e in tal caso richiedere informazioni in merito alla logica utilizzata nonché sulle conseguenze previste da tale trattamento.

Infine nei successivi paragrafi è previsto rispettivamente che: qualora i dati personali siano trasferiti verso un paese terzo o un’organizzazione internazionale, l’interessato ha diritto a essere informato in base al possesso, da parte dei soggetti suddetti, dei requisiti previsti dall’articolo 46 del Reg. che subordina il trasferimento dei dati, al di fuori dell’ombrello giuridico dell’Unione europea, alla sola condizione che siano previste adeguate garanzie sul trattamento; che il titolare fornisca una copia dei dati personali oggetto di trattamento, e che se la richiesta è presentata mediante l’utilizzo di mezzi elettronici (e qui la disposizione è figlia del suo tempo), salvo indicazione diversa dell’interessato, le informazioni devono essere fornite in un formato elettronico di uso comune.

In ogni caso come affermato più volte non essendo il diritto fondamentale alla protezione dei dati personali, e di conseguenza anche tutti i diritti ad esso sottesi, dei diritti assoluti anche le prerogative dell’interessato come i diritti d’accesso, d’informazione, di rettifica, di limitazione del trattamento ecc... soffrono delle limitazioni in base ad esigenze, spesso collettive o forse meglio dire pubbliche, ritenute prevalenti.

È quanto stabilisce infatti l’articolo 23 in tema di “Limitazioni” prevedendo che il diritto del’Unione e di uno Stato membro può limitare, mediante misure legislative, i diritti previsti nelle Sezioni 3 e 4 del Regolamento, se tale limitazione rispetti l’essenza dei diritti e delle libertà fondamentali e consista in una misura necessaria e proporzionata in una società democratica per

salvaguardare svariati interessi tra cui: la sicurezza nazionale, la difesa, la sicurezza pubblica o altri obiettivi di interesse pubblico generale specialmente per quanto riguarda l'aspetto economico e finanziario (politica monetaria, tributaria, sanità pubblica e sicurezza sociale). Oppure quando bisogna salvaguardare la tutela stessa dell'interessato o dei diritti e delle libertà altrui, l'indipendenza della magistratura e dei procedimenti giudiziari, nonché 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.

3.1. Il Diritto all'oblio

Il diritto all'oblio è senza dubbio un'altra delle grandi innovazioni che il Regolamento UE 2016/679 codifica e che entra a far parte definitivamente all'interno del sistema normativo del diritto alla protezione dei dati personali.
Dal 1995, con l'introduzione della Direttiva Madre, ad oggi il tema del diritto all'oblio e della cancellazione dei dati personali è stato al centro di vari interventi di grandissimo impulso creativo soprattutto derivanti dall'attività della Corte di Giustizia europea e dall'attività delle Autorità Garanti nazionali per la protezione dei dati personali dei vari Stati membri.
Va detto però che chi attendeva con trepidazione la "costituzionalizzazione" di istituti importanti come il diritto all'oblio, all'interno di un atto normativo europeo vincolante, generale e direttamente applicabile come il Regolamento, è rimasto non poco deluso dall'approssimazione minimalista del legislatore europeo. Infatti a molti è sembrato che il legislatore non abbia tenuto conto di tutti quegli sviluppi e sfaccettature che l'istituto del diritto all'oblio ha assunto nel tempo, appiattendolo fin troppo sul concetto di *erasure*, che anzi finiscono addirittura per coincidere. In questo modo il diritto alla cancellazione dei dati personali e il diritto all'oblio si traducono inevitabilmente nella volontà da parte del soggetto interessato della cessazione del trattamento dei dati personali,

confondendosi così, in un fumoso gioco di ombre, operazione materiale e finalità[91].

Come precisato poc'anzi da quando si è iniziato a parlare di diritto all'oblio fino alla famosa sentenza Google Spain del 2014, e infine con il Regolamento del 2016, quest'ultimo si è evoluto in diverse direzioni nel tempo e non tutte coincidevano con la cessazione del trattamento dei dati del soggetto interessato.

Infatti all'alba della nascita della nozione di oblio, quando nel panorama giuridico e sociale ancora non aveva irrotto con tutta la sua invasiva forza il web, la ricostruzione tradizionale della dottrina e della giurisprudenza si era consolidata prevalentemente su di una concezione di oblio come divieto di reiterazione della pubblicazione di una notizia, ormai datata nel tempo, e per cui l'interesse pubblico alla conoscenza di quel determinato fatto fosse svanito[92].

L'oblio, di conseguenza, era strettamente interconnesso con l'attività giornalistica e la riproposizione di fatti di cronaca, e perciò incidente con il diritto della stampa ad informare e dei cittadini a essere informati[93].

Questa primigenia concezione del diritto all'oblio come divieto di reiterazione di una notizia nel tempo, si colloca in una dimensione "*off-line*"[94], che differisce dalla dimensione *online* di cui parlerò a breve, principalmente per il ruolo che assume, all'interno della dinamica pubblicazione-violazione privacy, il fattore tempo.

---

[91] Come analizza G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità,* in *Diritto dell'Informazione e dell'Informatica*, cit., 2014, p.596 afferma che "*Volendo meglio delineare i confini di termini dal significato limitrofo, quali cancellazione dei dati e oblio 14, si può definire la cancellazione come un'operazione sui dati che esclude ogni ulteriore conservazione degli stessi, mentre l'oblio sembra piuttosto essere una finalità, che si può raggiungere con la cancellazione, ma anche con il blocco*."

[92] Si citano ad esempi, Cass., sez. I civ., 18 ottobre 1984, n.5259, in *Giur.it.*, 1985, c.762 ss; Trib. Roma 15 maggio 1995, in *Dir. Inf.*, 1996, p. 424 ss; Trib. Roma, ord. 27 novembre 1996, in *Dir. Aut.*, 1997, p.372 ss.

[93] Si veda per approfondimenti V. D'ANTONIO,"The right to tell people what they do not want to hear": *i moderni confini del diritto di fare informazione*, in V. D'ANTONIO – S.VIGLIAR, *Studi di diritto della comunicazione. Persone, società e tecnologie dell'informazione*, Padova, 2009, p.1 ss.

[94] Come definito da Virgilio D'Antonio, Professore ordinario di Diritto comparato dell'informazione, della comunicazione, Trademark and Advertising Comparative Law, all'Università di Salerno, che analizza l'evoluzione storica del diritto all'oblio da una dimensione *offline* ad una dimensione *online*. V. D'ANTONIO, "Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio *offline*", *Oblio e cancellazione dei dati nel diritto europeo*, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 203 ss.

Bisogna sottolineare comunque che questa concezione del diritto all'oblio è solo *de relato* riconducibile al diritto alla riservatezza in quanto non è trascurabile il fatto che in primis la pubblicazione della notizia è legittima, poiché riguardante fatti di cronaca e di pubblico interesse, e poi perché la pubblicazione della notizia originaria comporta di per sé la fuoriuscita di quel dato dalla sfera di riservatezza dell'individuo[95].

L'oblio, specificato in tal senso, tocca il diritto alla riservatezza nel momento in cui subentra nell'equazione il fattore tempo: ciò perché la notizia originaria, anche se legittimamente pubblicata, con il trascorrere del tempo perde di attualità e di utilità informativa per la società e di conseguenza non ne giustifica la reiterazione a distanza di tempo, con immediato richiamo alla violazione del diritto all'identità personale[96]. In ogni caso, stante la legittimità dell'originaria pubblicazione, il diritto all'oblio in questo caso non coincide con la cancellazione della notizia, ma incide esclusivamente sulla reiterazione di quest'ultima in un arco temporale differito e di conseguenza non vi è cessazione del trattamento.

Lo scenario muta completamente quando si parla di dimensione *on-line* del diritto all'oblio. Infatti il fattore temporale perde completamente la funzione di discriminante tra il momento della pubblicazione della notizia e quello di riproposizione della stessa, come accadeva nella dimensione *off-line*.

Il dato temporale risulta infatti appiattito su di un'unica linea in un contesto, come quello del Web, in cui non siamo più in presenza di momenti temporali separati e distinti (pubblicazione-reiterazione), ma in un continuo spazio-temporale dove la notizia permane in Rete dal momento dell'*upload* e che è consultabile da chiunque in qualsiasi momento. È chiaro che in una situazione di questo genere, dove manca una vera e propria riproposizione della notizia come nella dimensione *off-line*, non può più interpretarsi il diritto all'oblio come la pretesa dell'interessato affinché il fatto che lo riguarda, ormai datato nel tempo,

[95] *Ivi*, p. 204.
[96] *Ibidem.*

non sia soggetto a ingiustificate ripubblicazioni da parte di una testata giornalistica[97].

Variato il contesto, è dunque necessaria una variazione anche nell'interpretazione del diritto all'oblio in modo che la tutela dell'identità personale del soggetto interessato sia adeguata ed efficace all'interno delle nuove trame delineate dalla Rete.

In questo modo la vecchia concezione del diritto all'oblio, come divieto di ingiustificata riproposizione di un fatto datato concernente un determinato soggetto, si trasforma in una pretesa dello stesso soggetto affinché il fatto che lo riguarda sia "contestualizzato". Dunque l'informazione relativa alla persona non è rimossa dalla Rete, ma è aggiornata in modo tale da far sì che ciò che inevitabilmente permane sul web rispecchi la veridicità della situazione reale al di fuori.

Quindi il fattore temporale è appiattito, ma non annientato del tutto: infatti è tramite lo strumento dell'aggiornamento, previsto come un obbligo in capo al responsabile della pubblicazione, che il fattore tempo incide andando a mutare sul web, ciò che è mutato anche nella realtà.

Questa nuova accezione di diritto all'oblio come contestualizzazione del dato *on-line* è stato recepito con successo tanto dal Garante della privacy italiano, che più volte ha richiesto che negli archivi di quotidiani *on-line* fossero applicate varie operazioni di aggiornamento[98], quanto dalla giurisprudenza italiana.

Infatti la Corte di Cassazione italiana, sempre in tema di aggiornamento di archivi *on-line* di alcune testate giornalistiche nella famosa sentenza n. 5525 del 5 aprile 2012 ha fondato la sua decisione non sulla necessità che una certa notizia

---

[97] Come sottolineato da G. FINOCCHIARO, *ult. op. cit.*, p. 593 "*in Rete la ripubblicazione non è più necessaria, dal momento che per la stessa organizzazione dell'informazione nella Rete l'informazione non è cancellata, ma permane disponibile o quanto meno astrattamente disponibile. In altri termini, non si tratta solo o necessariamente di una ripubblicazione dell'informazione, ma piuttosto di una permanenza della stessa nella Rete. Muta dunque il ruolo che gioca il tempo e muta l'esigenza che si vuole soddisfare*."

[98] Si veda, GARANTE PROTEZIONE DATI PERSONALI, doc. web n. 2286820, 24 gennaio 2013; doc. web n. 1617673, 8 aprile 2009; doc. web n. 1583162, 11 dicembre 2008, in www.garanteprivacy.it.

sui motori di ricerca diventi irreperibile, ma piuttosto che venga aggiornata rispetto all'evolversi degli stessi fatti nel corso del tempo.

La questione riguardava la controversia instauratasi tra un politico arrestato per corruzione agli inizi degli anni '90, ma che fu in seguito prosciolto, e un quotidiano che negli archivi *on-line* deteneva la notizia dell'arresto, che dunque risultava ancora accessibile per chi ricercasse il documento, senza però che ci fosse alcun riferimento in merito all'esito positivo della vicenda processuale.

La Suprema Corte affermava che il diritto all'oblio, inteso come "contestualizzazione" *‹‹salvaguarda in realtà la protezione sociale dell'identità personale, l'esigenza del soggetto di essere tutelato dalla divulgazione di informazioni (potenzialmente) lesive in ragione della perdita […] di attualità delle stesse, sicché il relativo trattamento viene a risultare non più giustificato ed anzi suscettibile di ostacolare il soggetto nell'esplicazione e nel godimento della propria personalità».*

La Corte continua specificando che *«la notizia non può continuare a risultare isolatamente trattata e non contestualizzata in relazione ai successivi sviluppi della medesima […] giacché altrimenti la notizia, originariamente completa e vera, diviene non aggiornata, risultando quindi parziale e non esatta, e pertanto sostanzialmente non vera. […] Se vera, esatta ed aggiornata essa era al momento del relativo trattamento quale notizia di cronaca, e come tale ha costituito oggetto di trattamento, il suo successivo spostamento in altro archivio di diverso scopo (nel caso, archivio storico) con memorizzazione anche nella rete internet deve essere allora realizzato con modalità tali da consentire alla medesima di continuare a mantenere i suindicati caratteri di verità ed esattezza, e conseguentemente di liceità e correttezza, mediante il relativo aggiornamento e contestualizzazione. Solo in tal modo essa risulta infatti non violativa sia del diritto all'identità personale o morale del titolare, nella sua proiezione sociale, del dato oggetto di informazione e di trattamento, sia dello stesso diritto del cittadino utente a ricevere una completa e corretta informazione. Anche laddove come nella specie non si ponga una questione di tutela contro la diffamazione o*

di protezione dell'immagine o dell'onore, sussiste allora in ogni caso l'esigenza di salvaguardare il diritto del soggetto al riconoscimento e godimento della propria attuale identità personale o morale»[99].

Inoltre la Corte di Cassazione sottolinea la necessità di una costruzione dinamica della tutela alla riservatezza e dei dati personali, dove gli interessati sono al centro della tutela stessa, tramite lo strumento del controllo e dell'accesso alle informazioni che li riguardano detenute da altri affermando che *«l'interessato è divenuto compartecipe nell'utilizzazione dei propri dati personali.[…] La liceità del trattamento trova fondamento anche nella finalità del medesimo, quest'ultima costituendo un vero e proprio limite intrinseco del trattamento lecito dei dati personali, che fonda l'attribuzione all'interessato del potere di relativo controllo (tanto con riferimento alle finalità originarie che ai successivi impieghi), con facoltà di orientarne la selezione, la conservazione e l'utilizzazione. L'interessato ha diritto a che l'informazione oggetto di trattamento risponda ai criteri di proporzionalità, necessità, pertinenza allo scopo, esattezza e coerenza con la sua attuale ed effettiva identità personale o morale[…]Gli è pertanto attribuito il diritto di conoscere in ogni momento chi possiede i suoi dati personali e come li adopera, nonché di opporsi al trattamento dei medesimi, ancorché pertinenti allo scopo della raccolta, ovvero di ingerirsi al riguardo, chiedendone la cancellazione, la trasformazione, il blocco, ovvero la rettificazione, l'aggiornamento, l'integrazione»*[100].

In questo modo inoltre la Suprema Corte aggiunge un *quid pluris* alla concezione dell'oblio come contestualizzazione, prevedendo un vero e proprio obbligo per i gestori della pagina web di aggiornamento dei fatti conformi alla realtà, tutto ciò a garanzia della *web reputation* dell'individuo.

[99] Cass., sez. III civ., 5 aprile 2012, n. 5525, in *Foro it*, 2013, I, p. 305 ss con nota di A. TUCCI.
[100] *Ibidem.*

Anche in questo caso la concezione di oblio come contestualizzazione non prevede che il trattamento cessi e il materiale sia cancellato, ma che sia piuttosto accompagnato da ulteriori elementi d'aggiornamento[101].

Il significato di diritto all'oblio ha assunto un'ulteriore sfaccettatura esegetica grazie alla famosa sentenza della Corte di Giustizia Europea nella causa C-131/12 *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González.*

Nel 2009 il signor González lamentava, nello specifico, che dalla semplice immissione del suo nome all'interno del motore di ricerca fornito dalla società Google (*Google Search*), sarebbero stati facilmente reperibili contenuti lesivi della sua immagine, in quanto non esatti e non aggiornati.

I contenuti lesivi a cui si riferisce il sig. González erano contenuti in alcune pagine del famoso quotidiano spagnolo *La Vanguardia Ediciones SL* (alle quali il motore di ricerca rimandava), datate rispettivamente gennaio e marzo del 1998, nelle quali fu riportata come fatto di cronaca, una vendita all'asta di immobili organizzata a seguito di un pignoramento effettuato nei confronti del sig. Costeja González per la riscossione coattiva di crediti previdenziali.

A distanza di un arco temporale di dieci anni, nonostante la vicenda fosse risolta e l'utilità pubblica della notizia fosse ormai del tutto svanita il collegamento tra le pagine contenute nell'archivio *on-line* del quotidiano spagnolo e il motore di ricerca, risultava facilmente accessibile da parte di chiunque, tramite la semplice digitazione nella barra di ricerca del nominativo del sig. González.

Quest'ultimo allora richiedeva al quotidiano l'eliminazione delle informazioni che lo riguardavano in quanto, essendo la vicenda ormai chiusa e non essendo aggiornati i contenuti, sarebbero potute essere altamente lesive della sua immagine specialmente riguardo la sua affidabilità rispetto a futuri creditori.

[101] In tema, V. ZENO-ZENOVICH, *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985 e G. FINOCCHIARO, *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. Inf.*, 2012, p 383 ss.

Tuttavia, la testata spagnola riteneva di non poter da seguito alla richiesta del ricorrente in quanto la pubblicazione delle informazioni era stata voluta direttamente dal Ministro del Lavoro e degli Affari sociali.

L'interessato allora si rivolgeva direttamente a Google Spain S.L chiedendo la cancellazione dei dati che lo riguardavano e la deindicizzazione dei *link* che collegavano direttamente alle pagine del portale de *La Vanguardia* contenente le sue informazioni.

Anche Google Spain però respingeva tale richiesta puntualizzando che l'erogazione del servizio di motore di ricerca avveniva per opera della società Google Inc. avente sede in California.

Di conseguenza nel 2010 il signor Gonzales ricorreva direttamente di fronte l'Autorità Garante per la protezione dati spagnola nei confronti delle due società del gruppo Google richiedendo che i dati non aggiornati che lo riguardavano venissero cancellati.

In seguito, mentre l'*Agencia Española de Protección de Datos* respinse il reclamo diretto contro *La Vanguardia*, ritenendo che l'editore avesse legittimamente pubblicato le informazioni in questione, l'AEDP obbligava Google a rimuovere e/o occultare le informazioni controverse ed i relativi collegamenti, bloccandone anche la futura accessibilità tramite la deindicizzazione dei vari links.

La pronuncia dell'AEDP non fu accettata da Google Inc. che considerava la decisione applicata fuori dai confini territoriali e di conseguenza inapplicabile a Google Spain, poiché la Compagnia spagnola avrebbe svolto sul territorio dell'Unione solamente attività di tipo commerciale, mentre l'autentica attività di indicizzazione e trattamento dei dati personali sarebbe stata svolta, invece, da Google Inc., quest'ultima soggetta quindi alla legislazione californiana.

Nel 2012, la questione si spostò presso il Tribunale di Madrid (c.d. *Audiencia Nacionale*) in cui il colosso di Mountain View chiedeva al giudice la tutela del diritto alla libertà di espressione e informazione mentre il Garante spagnolo chiedeva la tutela del diritto all'oblio e alla privacy.

Il giudice nazionale spagnolo, una volta esaminato il caso, chiese il rinvio pregiudiziale dinanzi la Corte di Giustizia europea, al fine di individuare la norma di riferimento e saggiare la coerenza delle pretese avanzate dal Garante spagnolo e dal ricorrente.

I giudici della Corte europea addebitò a Google una responsabilità in merito a tutte e tre le questioni riportate.

Riguardo la questione della *territorialità* i giudici hanno disposto che, ai sensi della Direttiva 95/46/CE, Google Spain risponde a tutti i requisiti previsti dalla nozione di stabilimento ritenendo che «*il trattamento dei dati personali realizzato per le esigenze di servizio di un motore di ricerca come Google Search, gestito da un'impresa con sede in uno Stato terzo, ma avente uno stabilimento in uno Stato membro, viene effettuato nel contesto delle attività di tale stabilimento qualora quest'ultimo sia destinato a garantire in tale Stato membro la promozione e la vendita di spazi pubblicitari proposti dal suddetto motore di ricerca e che servono a rendere redditizio il servizio offerto da quest'ultimo*»[102]. Perciò le attività relative agli spazi pubblicitari, essendo gestite da Google Spain, si considerano a tutti gli effetti uno stabilimento della Google Inc.

In secondo luogo la Corte di Giustizia in merito alla questione della *responsabilità* del trattamento disponeva che l'attività posta in essere da un motore di ricerca e consistente nel «*trovare informazioni pubblicate o inserite da terzi su Internet, nell'indicizzarle in modo automatico, nel memorizzarle temporaneamente e, infine, nel metterle a disposizione degli utenti di Internet secondo un determinato ordine di preferenza, deve essere qualificata come "trattamento di dati personali", ai sensi del citato articolo 2, lettera b), qualora tali informazioni contengano dati personali, e che, dall'altro lato, il gestore di detto motore di ricerca deve essere considerato come il "responsabile" del trattamento*[103]». Dunque risulta chiaro l'assunto della Corte prevedendo che, nel

[102] Cfr. paragrafi da 45 a 61 sentenza citata.
[103] Cfr. paragrafi 21 e 41, sentenza citata.

caso in cui le informazioni contengano dati personali, le attività generalmente poste in essere da un motore di ricerca devono qualificarsi come una operazione di trattamento, discendendo da ciò che il motore di ricerca deve necessariamente ritenersi il responsabile dello stesso trattamento.

Così facendo la Corte risponde affermativamente anche al quesito posto dal giudice del rinvio quando si interrogava sulla possibilità che il ricorrente potesse riferirsi direttamente al motore di ricerca, invece che al soggetto che ha pubblicato l'informazione online[104], al fine di «*impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente*» e di conseguenza esercitando i diritti cancellazione, congelamento e opposizione direttamente nei confronti del motore di ricerca.

Infine per quanto riguarda la questione del diritto all'oblio richiesto dal sig. González, i giudici di Lussemburgo decisero che dato il trascorrere del tempo, che di per sé è capace di rendere un trattamento prima lecito, ora illecito a seguito di un'incompatibilità che « *può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario*[105]», ha previsto in capo al gestore del motore di ricerca l'obbligo di cancellare i collegamenti alle pagine elettroniche pubblicate dal soggetto terzo (il quotidiano *La Vanguardia*) riguardanti il pignoramento avvenuto anni prima,

[104] Infatti è la stessa Corte di Giustizia Europea a prevedere che il primo vaglio di fondatezza spetti proprio al gestore del motore di ricerca, quale diretto responsabile delle operazioni di trattamento. Quest'ultimo dovrà dunque ricercare il corretto equilibrio tra le istanze del ricorrente ed il legittimo interesse degli altri internauti. Il ricorrente, qualora veda disattesa la propria richiesta, potrà successivamente rivolgersi all'autorità di controllo per la protezione dati personali di riferimento o in alternativa direttamente all'autorità giudiziaria.

[105] Cfr. par . 92 sentenza citata.

ritenendosi, date le circostanze, il "diritto di essere dimenticati" prevalente sia sul diritto all'informazione che sugli interessi economici del motore di ricerca.

Dunque la Corte di Giustizia europea sembra aver contribuito ad aggiungere un'ulteriore sfumatura alla tavolozza di colori del diritto all'oblio, più che come diritto ad essere dimenticati, come "diritto a non essere trovati facilmente", tecnicamente inteso come diritto alla deindicizzazione delle informazioni[106].

Secondo questa interpretazione del diritto all'oblio, ciò che si persegue non è la totale eliminazione del dato personale dal web, ma piuttosto un oscuramento, se non una vera rimozione, dei sistemi di linkaggio tra le operazioni del motore di ricerca e il dato così come conservato, magari lecitamente, all'interno di archivi *on-line* di pagine web.

Come di fatto avvenuto nella vicenda Google Spain il ricorrente non ha ottenuto alla fine la rimozione del dato dal web (cosa tra l'altro molto difficile da attuare concretamente), ma piuttosto la deindicizzazione, intesa come una dissociazione del proprio nome da un determinato risultato di ricerca, rendendo così impossibile per il motore di ricerca ricollegare le due informazioni nuovamente e unirle tramite link.

In questa specifica declinazione il diritto all'oblio si traduce nella sottrazione al pubblico di una modalità di accesso semplificata e generalizzata ad informazioni sul proprio conto[107]. Per questo motivo non pare possibile ipotizzare istanze di rimozione di risultati di ricerca che vadano oltre la dissociazione di quella data pagina sorgente da quel determinato nome, sino a coprire tutte le possibilità di accesso alla pagina stessa mediante differenti modalità di interrogazione del motore di ricerca[108].

---

[106] In tema si rinvia a G. RESTA – V. ZENO-ZENOVICH, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015 e F. PIZZETTI, in *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, 2014.

[107] Così V. D'ANTONIO,"Il diritto all'oblio *on-line* come diritto alla deindicizzazione del dato", *Oblio e cancellazione dei dati nel diritto europeo*, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 212 ss.

[108] *Ivi* p. 213. Si veda inoltre, S. SICA – V. D'ANTONIO, *La procedura di de-indicizzazione,* 2015.

Questa concezione di oblio come deindicizzazione è quella che si avvicina di più all'interpretazione che sembra essere approcciata dal Regolamento 2016/679, se non perfettamente coincidente nella sostanza, lo è senz'altro per la finalità.

Abbiamo visto come le precedenti interpretazioni del diritto all'oblio non avevano come *target* finale quello della cessazione del rapporto di trattamento, anzi al contrario si presupponeva la continuazione del trattamento stesso al fine della concreta operabilità dell'oblio.

Nel caso invece dell'oblio come deindicizzazione, anche se non si prevede la cancellazione del dato come riportato dall'articolo 17 del nuovo Regolamento, la finalità è pur sempre coincidente con quella della disposizione regolamentare, e cioè la cessazione del trattamento imposta al titolare e/o al responsabile del trattamento.

Come detto in precedenza il significato di diritto all'oblio proposto dal Regolamento UE 2016/679 è un significato appiattito sulla concezione di *erasure* e cioè di cancellazione del dato personale da parte del titolare del trattamento con l'ulteriore conseguenza della cessazione del trattamento stesso.

Infatti il legislatore europeo accomuna in un'unica disposizione, pur menzionando in maniera distinta le due posizioni giuridiche, diritto alla cancellazione e diritto all'oblio trattandole in maniera congiunta in sede poi di determinazione del contenuto e della disciplina[109].

Questa tendenza si riscontra già da alcuni considerando introduttivi al testo normativo.[110]

Per esempio al considerando n. 65 si sottolinea che all'interessato deve essere garantito «*il diritto di chiedere che siano cancellati e non più sottoposti a trattamento i propri dati personali che non siano più necessari per le finalità per le quali sono stati raccolti o altrimenti trattati, quando abbia ritirato il proprio consenso o si sia opposto al trattamento dei dati personali che lo riguardano o quando il trattamento dei suoi dati personali non sia altrimenti conforme al*

[109] Si vedano F. PIZZETTI, *Il prisma del diritto all'oblio,* in *Il caso del diritto all'oblio*, Torino, 2013, p. 21 ss.

[110] Ci si riferisce rispettivamente ai considerando n. 65, 66, 67 Reg. citato.

presente regolamento.». Il considerando però prosegue prevedendo dei limiti al diritto dell'interessato qualora si riscontri la necessità della conservazione dei dati personali «*per esercitare il diritto alla libertà di espressione e di informazione, per adempiere un obbligo legale, per eseguire un compito di interesse pubblico o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento, per motivi di interesse pubblico nel settore della sanità pubblica, a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ovvero per accertare, esercitare o difendere un diritto in sede giudiziaria.*».

In effetti la posizione delineata nell'ultima parte del considerando n. 65, che prevede dei veri e propri limiti all'utilizzo del diritto all'oblio/cancellazione dei dati personali, è ripresa integralmente dal terzo paragrafo dell'articolo 17.

L'articolo 17 invece al primo paragrafo, oltre alla proclamazione del diritto in sé, enuncia le ipotesi specifiche affinché possa dirsi esistente un diritto all'oblio in capo all'interessato; ciò con il chiaro intento di circoscrivere l'ambito applicativo e di evitare che la posizione giuridica in questione si trasformi in una prerogativa incondizionata dell'interessato[111], dato il carattere estremamente pervasivo che tale diritto può assumere.

Dunque al primo paragrafo è rispettivamente previsto: da un lato, il diritto dell'interessato a ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo; dall'altro lato, l'obbligo per il titolare del trattamento di procedere alla cancellazione dei dati personali riferibili all'interessato senza ingiustificato ritardo, solo però se sussiste uno dei seguenti motivi:

a) i dati personali non sono più necessari rispetto alle finalità perle quali sono stati raccolti o altrimenti trattati;
b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9,

[111] V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo,* cit., p. 201.

paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento;

c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2;
d) i dati personali sono stati trattati illecitamente;
e) i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento;
f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1.

Infine al par.2 dell'articolo 17 è inserito un'ulteriore importante obbligo in capo al titolare del trattamento qualora abbia reso pubblici i dati personali e successivamente sia obbligato, ai sensi del par.1, a procedere alla cancellazione dei suddetti dati: infatti è previsto che «*tenendo conto della tecnologia disponibile e dei costi di attuazione* (il titolare) *adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali.*[112]».

Al di là di ogni dubbio si può dunque affermare che nell'impostazione proposta dal Regolamento europeo del 2016, diritto all'oblio e diritto alla cancellazione si sovrappongono[113], arrivando a coincidere quasi alla perfezione in termini sostanziali, e prevedendo la cessazione del trattamento dei dati personali ogni qualvolta risultino violati i principi di finalità, del consenso e di liceità del trattamento(tutti principi già codificati nella Direttiva 95/46/UE).

[112] Così, specificato anche nel considerando n. 66.
[113] Si veda V. D'ANTONIO, *Oblio e cancellazione dei dati nel diritto europeo,* cit., p. 220, dove afferma che "*la codificazione del diritto all'oblio proposta dal Regolamento europeo non rappresenta affatto lo stato dell'arte della materia ed, anzi, induce a ritenere che la storia di questa posizione giuridica ,lungi dall'aver raggiunti un punto d'arrivo,continuerà ad essere affidata più alle parole di corti e studiosi che a quelle dei legislatori (nazionali e sovranazionali).*".

3.2. Il Diritto alla portabilità dei dati personali

Un'altra delle rilevanti novità introdotte dal Regolamento del 2016 è costituita senz'altro dall'introduzione, nel catalogo dei diritti dell'interessato, del diritto alla portabilità dei propri dati personali descritta all'articolo 20.

Come specificato anche al considerando n. 68 il fine dell'introduzione di una disposizione come questa è di «*rafforzare ulteriormente il controllo sui propri dati è opportuno anche che l'interessato abbia il diritto, qualora i dati personali siano trattati con mezzi automatizzati, di ricevere in un formato strutturato, di uso comune, leggibile da dispositivo automatico e interoperabile i dati personali che lo riguardano che abbia fornito a un titolare del trattamento e di trasmetterli a un altro titolare del trattamento... Ove tecnicamente fattibile, l'interessato dovrebbe avere il diritto di ottenere che i dati personali siano trasmessi direttamente da un titolare del trattamento a un altro.*».

In questo modo si rende ancora più salda quell'interpretazione giurisprudenziale della Corte di Giustizia europea e della Corte di Cassazione[114], che ha sottolineato la necessità di una tutela dinamica della protezione dei dati personali in cui l'interessato riveste un ruolo sempre più attivo nelle dinamiche che riguardano il trattamento dei propri dati personali.

Affinché tale partecipazione possa realizzarsi «*È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati. Tale diritto dovrebbe applicarsi qualora l'interessato abbia fornito i dati personali sulla base del proprio consenso o se il trattamento è necessario per l'esecuzione di un contratto*.». Al contrario il diritto della persona alla portabilità dei propri dati «*Non dovrebbe applicarsi qualora il trattamento si basi su un fondamento giuridico diverso dal consenso o contratto. Per sua stessa natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari del*

[114] Si ricordano nello specifico le sentenze Cass., sez. III civ., 5 aprile 2012, n. 5525 e la causa C-131/12 *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González*.

trattamento che trattano dati personali nell'esercizio delle loro funzioni pubbliche.».

Ecco allora che la portabilità dei dati prevista all'articolo 20 si configura come il diritto da parte dell'interessato di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti a un titolare del trattamento; l'interessato ha inoltre diritto a trasmettere i dati che lo riguardano a un altro titolare del trattamento senza alcun impedimento da parte del titolare del trattamento cui li ha forniti qualora:

a) il trattamento si basi sul consenso ai sensi dell'articolo 6, par. 1, lettera a) (quando l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità), o dell'articolo 9, par. 2, lettera a) (quando in tema di dati personali c.d. sensibili l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1), o su un contratto ai sensi dell'articolo 6, par. 1, lettera b) (quando il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso); e
b) il trattamento sia effettuato con mezzi automatizzati.

È specificato inoltre al secondo paragrafo che la trasmissione dei dati da un titolare all'altro, se tecnicamente fattibile, può avvenire in via diretta, senza dunque che il passaggio di dati sia effettuata materialmente dall'interessato. Una possibilità di questo tipo costituisce senza dubbio un notevole risparmio in termini di economicità e rapidità delle procedure.

Infine agli ultimi due paragrafi (par. 3 e 4) è previsto che il diritto della persona alla portabilità dei propri dati non pregiudica in alcun modo l'operatività del diritto alla cancellazione (oblio) previsto all'articolo 17, e che il diritto alla portabilità non si applica a quelle categorie di trattamento necessarie all'esecuzione di un compito di interesse pubblico o altrimenti connesso

all'esercizio di pubblici poteri di cui è investito il titolare del trattamento, ovvero qualora sia in grado di ledere i diritti e le libertà altrui.

Il diritto alla portabilità dei dati senza dubbio è strettamente in relazione diretta con le dinamiche del mercato, terreno sul quale è destinato a operare e dove i dati sicuramente sono più suscettibili di essere soggetti ad abusi.

Il valore dei dati in termini economici e quanto ormai sia ricco, e quanto sarà ricco in futuro, il business della vendita dei dati personali è un tema molto ampio e connesso nel quale prudentemente non mi addentro, ma è un dato di fatto che oggigiorno, numerose sono le situazioni in cui una persona al fine di utilizzare un servizio può o necessariamente deve inserire i suoi dati *on-line*. E non si parla solamente delle proprie generalità, ma anche di categorie di informazioni più o meno sensibili come ad esempio i numeri di carte di credito.

I dati sensibili sono diventati sempre più un'autentica moneta di scambio in un mercato dove motori di ricerca, social network, operatori telefonici e siti di shopping online competono nel business della raccolta, della conservazione, dell'acquisto e dell'analisi di grandissime quantità di dati, al fine di individuare veri e propri modelli di comportamento sociale, suddividendo la popolazione in categorie di utenti, utilizzabili in diversi modi come per esempio per gli studi di mercato o in una campagna elettorale[115].

Ecco dunque che in mercato "sano", onde evitare situazioni di abuso, deve essere garantita la facoltà all'utente di poter cambiare servizio facilmente, portando via con sé i propri dati da un gestore all'altro come accade di norma quando si cambia un gestore telefonico; ciò dovrebbe potersi realizzare anche da un *service provider* all'altro, come nel caso dei social network[116].

In questo modo i dati non sarebbero più "ostaggio" dei fornitori di servizi *on-line* e chi volesse cambiare fornitore avrebbe la possibilità di portare con sé la propria

[115] P. PACILEO, *Il diritto alla portabilità*, Cap. XI, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 227.
[116] *Ivi,* p. 237.

storia digitale e riprendere il cammino con un nuovo gestore esattamente al punto dove lo aveva interrotto con il vecchio[117].

Tanto il Legislatore europeo, quanto il Gruppo di Lavoro comune ex articolo 29 hanno sottolineato la necessità, affinché il sistema della portabilità funzioni adeguatamente, dell'implementazione di formati interoperabili[118] tra i vari fornitori di servizi, al fine di facilitare la trasmissione dei dati ed evitare situazioni di "*lock-in*" dei dati.

Nelle linee guida elaborate in tema di portabilità dei dati (WP 242)[119], il Gruppo art. 29, ricordando che all'articolo 20, par. 2, è previsto l'obbligo da parte del titolare del trattamento di trasmettere direttamente i dati al nuovo titolare, se tecnicamente fattibile[120], specifica che «*L'aspettativa è che il titolare trasmetta i dati personali in un formato interoperabile, ma ciò non configura alcun obbligo in capo agli altri titolari di supportare tale formato. Pertanto, la trasmissione diretta dei dati da un titolare all'altro potrebbe avvenire se è possibile instaurare una comunicazione fra due sistemi, in modo sicuro*[121]*, e se il sistema ricevente è tecnicamente in grado di ricevere i dati in ingresso.*»; e ancora prosegue affermando che in prima persona «*il WP29 sostiene con forza la ricerca di forme di collaborazione fra i produttori e le associazioni di categoria che soddisfino i requisiti del diritto alla portabilità dei dati.*».

Dunque interoperabilità dei sistemi tra fornitori e standardizzazione dei personal data sono le chiavi di volta affinché il diritto alla portabilità possa operare con successo e con le garanzie necessarie a proteggere i dati personali degli utenti digitali.

---

[117] *Ivi*, p. 240.

[118] Lo standard ISO/IEC 2382-01 definisce l'interoperabilità come segue: "*La capacità di comunicare, eseguire programmi o trasferire dati fra diverse unità funzionali in una modalità che richiede all'utente conoscenze minime o nulle delle caratteristiche peculiari di tali unità*".

[119] GRUPPO DI LAVORO COMUNE EX ARTICOLO 29, *Linee-guida sul diritto alla "portabilità dei dati"*, 13 dicembre 2016 Versione emendata e adottata il 5 aprile 2017, WP 242, 2017.

[120] Si ricorda in ogni caso che secondo quanto specificato anche nel Considerando n.68 " *Il diritto dell'interessato di trasmettere o ricevere dati personali che lo riguardano non dovrebbe comportare l'obbligo per i titolari del trattamento di adottare o mantenere sistemi di trattamento tecnicamente compatibili.*"

[121] Tramite ad esempio comunicazione autenticata con il livello adeguato di cifratura.

4. Controller e Processor

Il Regolamento 2016/679 dedica molta attenzione al Capo IV che, come sottolineato più volte, è uno dei principali veicoli d'introduzione di alcune notevoli innovazioni all'interno della disciplina della protezione dei dati personali, o quantomeno è sicuramente espressione di quel cambio di rotta per cui ha optato il legislatore del 2016, e che rappresenta una delle principali differenze di fondo con la Direttiva del '95, per cui il centro del sistema di tutela dei dati personali sarebbe traslato dai diritti dell'interessato, al complesso di norme che regolano, da una parte, il trattamento dei dati e le rispettive misure di sicurezza da adottare in un'ottica preventiva - precauzionale, dall'altra la serie di norme relative ai doveri e agli obblighi dei soggetti che partecipano al trattamento (titolare - responsabile). L'importanza che il legislatore ripone alle regole incentrate sui doveri del *controller* e del *processor*, considerando la corretta osservanza di quest'ultime un presupposto fondamentale per l'esercizio dei diritti dell'interessato, ancor prima, che per la tutela del diritto alla protezione dei dati personali, si intuisce da una rapida analisi della struttura regolamentare.
Si nota facilmente infatti che il Capo IV è uno dei blocchi normativi della nuova disciplina più ampi, suddiviso in ben cinque sezioni.
Il Capo IV intitolato "*Titolare del trattamento e responsabile del trattamento*" si apre con l'articolo 24 che, quasi con un bisticcio di parole, parla di "Responsabilità del titolare del trattamento"[122].
Il titolare, così come descritto all'articolo 4 del Regolamento (Definizioni), è quel soggetto (persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo) che determina le modalità, le finalità e le scelte operative in merito al trattamento dei dati e che in tal modo si pone al vertice della piramide dei soggetti del trattamento.

[122] G. M. RICCIO, *Data Protection Officer e altre figure*, Cap. III, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 41.

L'articolo 24 prevede espressamente che il titolare del trattamento adotti le misure tecniche e organizzative adeguate in modo tale da garantire, ed essere capace di dimostrare, che le operazione da lui poste in essere durante il trattamento siano conformi alle disposizione del regolamento. Il titolare pone in essere tali misure solamente dopo aver valutato la natura, l'ambito d'applicazione, il contesto e le finalità del trattamento, nonché dopo aver sondato preventivamente quali siano i rischi, in termini di probabilità e gravità, per i diritti e le libertà delle persone fisiche.

All'ultimo paragrafo inoltre è previsto che l'adesione ai codici di condotta (art. 40 Reg.) e/o ai meccanismi di certificazione (art. 42 Reg.), può essere utilizzata dal titolare del trattamento come un elemento probatorio per dimostrare il rispetto degli obblighi e la conformità del suo operato alle disposizioni regolamentari. Risulta maggiormente delineato un centro di imputazione della responsabilità ritagliato sulla figura del titolare del trattamento a titolo oggettivo, o come affermato da parte di autorevole dottrina semi-oggettivo[123].

Il legislatore, a ben vedere, sembra optare per un approccio improntato non alla riparazione dell'illecito, ma a quello della prevenzione del danno; ciò sarebbe

[123] Il richiamo è all'articolo 15 del d.lgs 30 giugno 2003 n 196 (Codice della Privacy). In base al I comma di tale norma prevede che "*chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'art. 2050 del codice civile*."
Come affermato da L. MODAFFARI, *La responsabilità per illecito trattamento dei dati personali,* in http://www.overlex.com, 2008, l'avvocato spiega che "*In forza della disposizione de qua il Legislatore ha specificato un'ulteriore ipotesi di applicazione della figura di responsabilità per attività pericolosa ex art. 2050 c.c., la quale prevede una responsabilità aggravata, di tipo oggettivo o semioggettivo, nei confronti di chi svolge una attività pericolosa. Il richiamo alla figura ex art 2050 c.c. è oggetto di vivace dibattito dottrinale. Sul punto vi sono due contrapposti orientamenti:*
1) *In base ad un primo, il richiamo a tale norma ha l'effetto di qualificare il trattamento dei dati personali come vera e propria attività pericolosa. Tale tesi si basa sia su considerazioni di ordine generale che su ulteriori dati normativi previsti dal Codice della Privacy stesso. Infatti, alla luce dell'intera disciplina del trattamento dei dati personali, il concetto di "attività pericolosa" si fonda sulla necessaria esigenza di tutelare la riservatezza, l'identità personale e il diritto alla protezione dei dati personali. Pertanto, l'attività di trattamento degli stessi deve necessariamente essere posta in essere nel rispetto del principio di legalità, correttezza e in modo anonimo. A riprova di ciò, il Legislatore, dagli art. 31 e seguenti Codice della Privacy, prevede dei veri e propri obblighi di sicurezza, tramite i quali si vuole evitare che "i rischi di distruzione o di perdita, anche accidentale, dai dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta"*.
2) *Altri Autori, invece, ritengono che il richiamo all'ipotesi ex art 2050 c.c. sia solo un "escamotage" per consentire al soggetto leso una regola probatoria di favore. Tramite il richiamo alla figura de qua, il Legislatore ha voluto solo prevedere una inversione nell'onere probatorio per tutelare maggiormente il soggetto leso, il quale sarà tenuto solo a dimostrare il danno subito ed il nesso di causalità*.".

confermato anche dal fatto che la disposizione manca di un'elencazione tassativa dei compiti e delle attività che il titolare del trattamento deve porre in essere, ma si predilige piuttosto l'analisi del rischio e degli eventuali danni causati, per cui il titolare ha l'obbligo di predisporre «*misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento.*[124]».

Dunque già dalla definizione di titolare del trattamento, e delineate le linee guida della sua responsabilità, si possono intuire i fondamentali aspetti su cui sono incentrati il trattamento e le azioni dell'agente principale, che di fatto decide le modalità e le finalità con cui porlo in essere, e che corrispondono con alcune delle novità più importanti di questo capo: come il determinante ruolo che assumono le misure di sicurezza, la tutela a carattere preventivo, la valutazione dei rischi e dei danni in un momento anteriore rispetto all'applicazione delle operazioni del trattamento.

Il Regolamento inoltre prende in considerazione il Contitolare del trattamento, inserendolo autonomamente come figura all'articolo 26.

Tale figura in realtà era già richiamata indirettamente dalla Direttiva 95/46/CE quando analizzando la figura del Responsabile (ora Titolare), stabiliva che quest'ultimo fosse «*la persona fisica o giuridica(...)che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*.[125]».

La contitolarità di un trattamento ricorre allorché due o più titolari determinano congiuntamente le finalità e i mezzi del trattamento. In questo modo si è in presenza di due titolari del trattamento aventi entrambi poteri decisionali, anche se congiuntamente, distinguendosi in maniera netta dalla figura del responsabile che, al contrario, non ha poteri decisionali rispetto ai dati personali e che agisce esclusivamente su indirizzo del titolare stesso.

È inoltre previsto in capo ai due o più titolari l'obbligo di determinare mediante un accordo e in modo trasparente, la ripartizione delle rispettive responsabilità in

[124] Così articolo 24, par.1, Regolamento UE/2016/679.
[125] Articolo 2, lett. d), Direttiva 95/46/CE.

merito all'osservanza degli obblighi derivanti dal Regolamento, specialmente per quanto riguarda l'esercizio dei diritti dell'interessato e delle comunicazioni delle informazioni per quest'ultimo. Dunque nell'accordo sono individuati, nella maniera più chiara possibile, i rispettivi ruoli e i rapporti tra contitolari e interessati, essendo previsto inoltre che il contenuto essenziale dell'accordo sia messo a disposizione dell'interessato[126].

Non solo, è previsto infine al paragrafo terzo dell'articolo 26, con grande *favor* per il soggetto interessato, che quest'ultimo, indipendentemente dal contenuto dell'accordo fra contitolari, possa esercitare i propri diritti liberamente nei confronti di ciascuno dei titolari del trattamento.

In chiusura della Sezione I troviamo altre due disposizioni che rimandano ad obblighi del titolare rispettivamente agli articoli 30 e 31.

All'articolo 30 è previsto in capo al titolare, e quando possibile al suo rappresentante, l'obbligo di tenuta di un registro delle attività di trattamento svolte sotto la propria responsabilità. Quest'obbligo ha senza dubbio lo scopo, più che di un'autentica protezione dell'interessato, di facilitare il controllo da parte delle autorità garanti, qualora richiedano ai titolari chiarimenti in merito ai trattamenti operati.

Il registro deve contenere necessariamente tutte le seguenti informazioni:

a) il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
b) le finalità del trattamento;
c) una descrizione delle categorie di interessati e delle categorie di dati personali;
d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;

[126] Così articolo 26, par. 2, Reg. citato.

e) ove applicabile, i trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale, compresa l'identificazione del paese terzo o dell'organizzazione internazionale e, per i trasferimenti di cui al secondo comma dell'articolo 49, la documentazione delle garanzie adeguate;
f) ove possibile, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
g) ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1.

Infine in maniera alquanto lapidaria all'articolo 31 intitolato "*Cooperazione con l'autorità di controllo*" è previsto l'obbligo generale per il titolare, il responsabile e quando previsto del loro rappresentante, di cooperare con l'autorità di controllo nell'esecuzione dei suoi compiti, qualora ne faccia richiesta.

Il Responsabile del trattamento invece è individuato, sempre a norma dell'articolo 4, n. 8 del Regolamento, nella «*persona fisica o giuridica(…)che tratta dati personali per conto del titolare del trattamento*».

Il responsabile, va detto, si configura come un soggetto eventuale, nel senso che il titolare ricorre ai servizi del responsabile qualora sia indispensabile e il trattamento «*debba essere effettuato per conto del titolare del trattamento*». A tal proposito l'articolo 28, al primo paragrafo, specifica che il titolare ricorre unicamente al servizio di quei responsabili che presentino garanzie sufficienti per mettere in atto quella serie di misure tecniche e organizzative che siano adeguate al soddisfacimento dei requisiti regolamentari e alla tutela dei diritti degli interessati.

È previsto inoltre che il rapporto tra titolare e responsabile, nonché i trattamenti ad opera di quest'ultimo, siano disciplinati direttamente da un contratto o altro atto giuridico, stipulati in forma scritta ovvero in forma elettronica (combinato par. 3 e 9, art. 28), che vincoli il responsabile al titolare e che stabilisca rispettivamente: la materia disciplinata, la durata, la natura e la finalità del

trattamento, la tipologia di dati personali e la categoria di interessati, gli obblighi e i diritti del titolare del trattamento.

Il responsabile dunque ha una funzione prevalentemente di supporto in ordine alle funzioni e mansioni del titolare, facendo strettamente riferimento alle disposizioni del titolare derivanti dal contratto. La funzione di supporto si ricava direttamente dal paragrafo 3 dell'articolo 28 quando si specifica che il responsabile del trattamento: assiste, tenendo conto della natura del trattamento, il titolare predisponendo le misure tecniche e organizzative adeguate per soddisfare l'obbligo del titolare di dare seguito alle richieste d'esercizio dei diritti da parte dell'interessato (lett. e); assiste il titolare per garantire il rispetto degli obblighi di cui agli artt. 32 a 36, tenendo sempre conto della natura del trattamento e delle informazioni a disposizione (lett. f); cancella o restituisca a scelta del titolare i dati personali dopo che sia terminata la prestazione dei servizi, salvo che la conservazione non sia disposta dal diritto dell'Unione o di uno Stato membro (lett. g); infine, mette a disposizione del titolare le informazioni necessarie per la conferma del rispetto delle disposizioni regolamentari oppure consenta e/o contribuisca ad attività di revisione e ispezione realizzate dal titolare o su ordine di quest'ultimo.

È prevista dal Regolamento, inoltre, la possibilità per il responsabile di ricorrere a un altro responsabile, previa autorizzazione scritta, specifica o generale, da parte del titolare. Anche in questo caso si instaura un rapporto tra responsabile e sub-responsabile di natura contrattuale, come tra titolare e responsabile, avente i medesimi contenuti dell'accordo di cui al par. 3; l'unica nota di distinzione è riscontrabile nell'eventualità in cui l'altro responsabile ometta di adempiere ai propri obblighi specifici in materia di protezione dati: in questo caso ricadrà comunque sul responsabile iniziale l'intera responsabilità dell'adempimento nei confronti del titolare del trattamento[127].

[127] Così come stabilito dalla decisione della Commissione europea del 5 febbraio 2010, n. 2010/87/UE – 27 maggio 2010, in cui si ammette la possibilità che l'importatore, tramite subcontratto assegni a terzi l'esecuzione, parziale o totale, degli obblighi assunti con l'esportatore, previo consenso scritto di quest'ultimo. Tuttavia a fronte di un subcontratto, "*Nell'ipotesi poi che il sub-incaricato non adempia*

Altre previsioni interessanti si riscontrano ai paragrafi 7 e 8 dell'articolo 28.

Entrambi i paragrafi prevedono la possibilità, da parte di due tipologie di soggetti esterni al trattamento, rispettivamente la Commissione e l'Autorità di controllo competente, di adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 dell'articolo, e cioè quelli che prevedono i contenuti degli accordi tra titolare e responsabile e tra responsabile e sub-responsabile.

La Commissione può stabilire tali clausole tipo secondo la procedura prevista dall'articolo 93, paragrafo 2 del Regolamento, che fa esplicito richiamo alla procedura di comitato e, nello specifico, al combinato disposto degli artt. 5 e 8 del regolamento UE 2011/182[128].

L'Autorità di controllo invece stabilisce tali clausole contrattuali in conformità del meccanismo di coerenza previsto all'articolo 63[129] del Regolamento.

La previsione di clausole tipo da parte di soggetti esterni al rapporto di trattamento sicuramente comporta una forte limitazione dell'autonomia contrattuale privata, anche se come asserito da autorevole dottrina[130], fonti di eterointegrazione della volontà contrattuale, possono comportare nell'ambito della protezione dei dati personali notevoli sgravi per le imprese, sotto il punto di vista di un risparmio dei costi d'attuazione e di conformazione al dettato

---

agli obblighi contemplati dal contratto, l'importatore deve rimanere responsabile nei confronti dell'esportatore". GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Decisione Commissione, clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi*, dir. 95-46-CE - 5 febbraio 2010, pdf, in www.garanteprivacy.it.

[128]Il regolamento UE/2011/182 stabilisce le regole e i principi generali relativi alle modalità di controllo da parte degli Stati membri dell'esercizio delle competenze di esecuzione attribuite alla Commissione e prevede all'articolo 5 la *Procedura d'esame*, mentre l'articolo 8 disciplina gli *Atti immediatamente applicabili.* Per una visione completa della normativa Regolamentare si rinvia a Regolamento (UE) n. 182/2011 del Parlamento europeo e del Consiglio, del 16 febbraio 2011, consultabile all'indirizzo www.eur-lex.europa.eu.

[129] Il legislatore dedica un'intera sezione alla Coerenza e in apertura di sezione, all'articolo 63 intitolato "*Meccanismo di coerenza*", stabilisce che al fine di contribuire all'applicazione del regolamento le autorità di controllo cooperano tra loro e con la Commissione, quando è richiesto, mediante il meccanismo di coerenza, così come stabilito nelle disposizioni successive, presenti nella sezione II del Capo VII (*Cooperazione e coerenza*).

[130] Stefano Rodotà afferma che ormai da tempo la sostituzione dell'autonomia contrattuale da parte di fonti di integrazione non opera solamente dove vi siano lacune dell'ordinamento, oppure dove il regolamento contrattuale sia inidoneo ad operare o altrimenti improduttivo di effetti, ma agiscono come forme di eterointegrazione della stessa volontà contrattuale. S. RODOTÀ, *Le fonti di integrazione del contratto*, Milano, 1969.

normativo europeo, essendo possibile ricorrere direttamente ad uno schema tipo di per sé fedele ai dettami normativi regolamentari.

Come sostenuto da autorevole dottrina, non siamo in presenza di una clausola da sostituire perché contraria ad una prescrizione normativa, né in presenza di una *default rule*, ma al più la fattispecie in esame può essere accostata alle *immutable rules* americane, pensate dalla dottrina USA, per utelare non solo le parti del contratto, quanto i terzi, la cui sfera giuridica potrebbe essere lesa dagli effetti o dall'esecuzione del contratto stesso[131].

Il Regolamento, poi dedica un'intera sezione (la quarta del Capo IV) alla nuova figura del *Data Protection Officer*. Il DPO, ovvero il Responsabile della protezione dei dati, secondo la nomenclatura italiana, che non risparmia anche in questo casi dubbi e incomprensioni nei termini utilizzati, è senza dubbio una delle novità più grandi inserite dal Regolamento n. 679/2016.

La figura del *Protection Officer* è istituto già noto nel mondo anglosassone, specialmente in quello delle multinazionali americane[132], nonché in alcuni ordinamenti europei dove già sono state introdotte figure similari[133] come Germania, Austria e Repubblica Ceca.

Dunque tramite l'emanazione del Regolamento, data la sua generale applicabilità e la sua efficacia diretta esplicata verso ogni ordinamento nazionale degli Stati membri, per la prima volta entra in pianta stabile nell'ordinamento comunitario la figura del Data Protection Officer, che diventerà agente costante e molto importante per la protezione dati degli individui, e che si aggiungerà al novero dei soggetti che operano all'interno del procedimento di trattamento dei dati personali, insieme al titolare e responsabile.

---

[131] In termini pressoché testuali G. M. RICCIO, *Data Protection Officer e altre figure,* cit., pag. 49.

[132] Cfr. F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali* , Torino, 2016, p. 155.

[133] Il riferimento è al *datenschutzbeauftragter* introdotto con il *Bundesdatenschutzgesetz* del 2003 e con il quale il responsabile della protezione dei dati sembra presentare svariate analogie come: l'obbligo di nomina in base ad un numero minimo di dipendenti (secondo l'originaria formulazione dell'art. 37che sembra essere stata espunta dal dettato normativo), la possibilità per il DSB di avere accesso a tutte le informazioni relative ai trattamenti, il divieto di penalizzare il DSB per le funzioni esplicate in base al ruolo che riveste e l'approccio, derivante dal modello tedesco, di *corporate self-monitoring* dove sono le società che direttamente si fanno carico di un adeguamento e di uno scrupoloso controllo nella gestione dei dati personali. G. M. RICCIO, *Data Protection Officer e altre figure,* cit., pag. 50-51.

L'articolo 37 espone al primo paragrafo i casi in cui sistematicamente si rende necessaria la nomina da parte del titolare e del responsabile del trattamento del DPO e cioè quando:

a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;
b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; oppure
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9 (si fa riferimento alla categoria dei c.d. dati sensibili) o di dati relativi a condanne penali e a reati di cui all'articolo 10.

Il *Data Protection Officer* si configura dunque come una figura estremamente garantista a tutela degli interessi e diritti delle persone fisiche, la cui necessità di nomina (intesa come un vero obbligo gravante sul titolare del trattamento) è prevista in quei particolari settori, a carattere prevalentemente pubblicistico o dove categorie di dati più o meno sensibili vengono trattati, ma non solo: infatti la nomina può essere necessaria anche qualora le attività del titolare trattino dati personali su larga scala[134], richiedendo altresì il monitoraggio[135] costante e sistematico degli interessati.

[134] Il Regolamento non dà una definizione del termine "larga scala". A tal proposito di grande utilità sono state le *Linee-guida sui responsabili della protezione dei dati (RPD)* adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), dove il Gruppo Articolo 29 ha fornito ampie delucidazioni interpretative e chiari esempi a supporto. Il gruppo fornisce dei criteri per capire quanto un trattamento sia applicato su larga scala e sono: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; 1) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; 2) la durata, ovvero la persistenza, dell'attività di trattamento; 3) la portata geografica dell'attività di trattamento.
Gli esempi di trattamenti su larga scala che il Gruppo riporta sono:1) trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività; 2) trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio); 3) trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità

Oppure come specificato al paragrafo 4, qualora sia previsto dal diritto dell'Unione o da una previsione normativa di uno Stato membro, nel caso in cui il titolare e il responsabile del trattamento, nei casi diversi dal paragrafo 1, volontariamente possono designare un responsabile della protezione dei dati personali.

Il responsabile dei dati personali è una figura altamente tecnica e professionale che è scelta in base alla conoscenza specifica della normativa e della prassi in tema di protezione dei dati personali e in base alla capacità di assolvere ai compiti previsti dall'articolo 39 del Regolamento.

---

statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food; 4) trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività; 5) trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale; 6) trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici. GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, le *Linee-guida sui responsabili della protezione dei dati (RPD)* adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), WP 243, 2016.

Bisogna sottolineare comunque come il Considerando n. 91 del Regolamento in realtà fornisca un abbozzo dei criteri per definire il concetto di trattamenti su larga scala identificandoli come quelli che "*mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato*". Continua poi prevedendo che "*Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato*".

[135] Come per il concetto di larga scala anche quello di *monitoraggio regolare e sistematico* non trova un'esplicita spiegazione all'interno della disposizione regolamentare. Sempre all'interno delle linee guida predisposte dal Gruppo di lavoro art. 29 sono forniti esempi riguardo ciò che il Gruppo intende per "regolare" e "sistematico". L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del WP29: 1) che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito; 2) ricorrente o ripetuto a intervalli costanti; 3) che avviene in modo costante o a intervalli periodici. L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29: 1) che avviene per sistema; 2) predeterminato, organizzato o metodico; 3) che ha luogo nell'ambito di un progetto complessivo di raccolta di dati; 4) svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc. GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, le *Linee-guida sui responsabili della protezione dei dati (RPD)* adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), WP 243, 2016.

È previsto inoltre che il DPO possa essere anche un dipendente del titolare o del responsabile del trattamento, o in alternativa essere assunto in base ad un contratto di servizi; ad ogni modo incombe sul titolare l'obbligo di pubblicare i dati di contatto del *privacy officer* e di comunicarli all'autorità di controllo (par. 6 e 7, art. 37.

Ulteriori importanti disposizioni in merito al soggetto del responsabile della protezione dati sono contenute all'articolo 38 denominato "*Posizione del responsabile della protezione dei dati*".

Innanzitutto è previsto che il *Data Protection Officer* sia coinvolto tempestivamente e adeguatamente in tutte le questioni riguardante la protezione dei dati durante il trattamento e, al fine di garantirne l'autonomia e l'indipendenza, che sia sostenuto direttamente dal titolare e dal responsabile che hanno il compito di fornire le risorse necessarie al responsabile della protezione dati per assolvere i suoi compiti e mantenere la propria conoscenza specialistica. Inoltre, sempre per i fini di cui ho appena parlato, è previsto che il Data Protection Officer mantenga rapporti direttamente con il vertice gerarchico del trattamento (titolare o al posto suo il responsabile) in modo tale da evitare rapporti diretti con altri soggetti ed evitare che così aumentino gli eventuali centri di imputazione della responsabilità nel caso in cui si verifichi un illecito riferibile al trattamento e infine che il DPO non sia rimosso o penalizzato per aver adempiuto ai propri compiti.

Il responsabile della protezione dati si configura poi come un soggetto intermedio tra titolare e interessato e tra titolare e autorità di controllo. Infatti una funzione molto importante del *Data Officer*, data anche l'autonomia e l'indipendenza di cui gode, è quella di essere un utile referente per le autorità garanti, ma soprattutto per gli interessati, che finalmente vedono abbattersi il "muro" rappresentato dalla struttura dentro il quale opera il titolare, trovando un diretto riscontro alle proprie istanze nella persona del *Data Protection Officer*.

Ciò è ricavabile direttamente dal dettato normativo quando al par. 4 dell'articolo 38 il Regolamento prevede che «*Gli interessati possono contattare il*

responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento.».

Per quanto riguarda, invece, la funzione di cooperazione del DPO con le autorità di controllo, l'articolo 39 intitolato "*Compiti del responsabile della protezione dei dati*" prevede alla lettera d) che il responsabile è incaricato in linea generale di «*cooperare con l'autorità di controllo*», mentre alla successiva lettera e) di «*fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.*».

Ulteriori compiti previsti dall'articolo 39, oltre al generale obbligo di considerare ai fini del trattamento, i rischi inerenti, la natura, l'ambito d'applicazione, il contesto e le finalità, il responsabile della protezione dati è incaricato inoltre di:

a) informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
b) sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo;
c) fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35.

Per il Gruppo di Lavoro ex. Articolo 29 la nomina di un *Data Protection Officer* è importante in quanto questa figura rappresenta un elemento fondante ai fini

della responsabilizzazione. La stessa presenza del DPO può facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese, nel rispetto del principio di *accountability.*

Il Gruppo ricorda, inoltre, che il responsabile della protezione dati svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del Regolamento quali i principi fondamentali del trattamento, i diritti degli interessati, la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento, la sicurezza dei trattamenti e la notifica e comunicazione delle violazioni di dati personali.

Pertanto i Garanti europei consigliano che la presenza del *Data Protection Officer* sia l'approccio standard all'interno della struttura del titolare e del responsabile, prevedendo inoltre, la necessità che il DPO partecipi ai gruppi di lavoro che si occupano delle attività di trattamento, all'interno della struttura suddetta[136].

5. Le misure di sicurezza: violazione dei dati personali (*data breach)*, notifica all'autorità di controllo e comunicazione all'interessato

È concezione ormai condivisa che il trattamento dei dati personali sia da qualificarsi come un'attività rischiosa, da cui consegue come necessario corollario l'esigenza di vagliare con grande attenzione quella serie di rischi connessi alle varie attività di trattamento, al fine di garantire nella maniera più completa ed efficiente una protezione ai dati personali degli individui[137].

[136] M. Iaselli, *I compiti del Data Protection Officer: chiariamo tutti i dubbi,* 21 aprile 2017, in www.agendadigitale.eu.

[137] Tali rilievi furono portati alla luce già in sede di dibattito della proposta di Regolamento della Commissione, davanti al Parlamento europeo e al Consiglio, al quale si rimanda COMMISSIONE EUROPEA, *Salvaguardare la privacy in un mondo interconnesso – Un quadro europeo della protezione dei dati per il XXI secolo,* COM (2012), 25 gennaio 2012; si veda inoltre ARTICLE 29 DATA PROTECTION WORKING PARTY, *Statement on the role of a risk-based approach in data protection legal frameworks* (WP 218), 30 maggio 2014.

All'interno della nuova disciplina della protezione dei dati personali, predisposta dal Regolamento UE/2016/679, riveste un ruolo importantissimo l'apparato di norme relative alla misure di sicurezza.

Infatti il nuovo Regolamento affronta con molta attenzione i temi delle misure di sicurezza da applicare, ma soprattutto presta grande attenzione alla valutazione e alla gestione del rischio, in modo tale da apportare una tutela efficace in maniera preventiva e non solamente successiva. A supporto di una concezione di prevenzione del rischio e del danno per la tutela delle persone fisiche e dei dati che le riguardano, sono predisposti numerosi strumenti di cui i più innovativi all'interno del Capo IV sono senz'altro, oltre i vari regimi di comunicazione e notificazione in caso di avvenuta violazione dei dati personali, la valutazione d'impatto, la consultazione preventiva e l'elaborazione dei concetti di *privacy by design* e *privacy by default.* Il legislatore comunitario, dunque, ravvisa nella prevenzione del rischio l'obiettivo primario al quale deve indirizzarsi ogni attività di trattamento e le disposizioni sulle misure di sicurezza costituiscono quel livello minimo essenziale di precauzione al quale il titolare, o chi per lui, deve attenersi.

L'articolo 32 intitolato "*Sicurezza del trattamento*" apre la Sezione II del Capo IV concernente la sicurezza dei dati.

Anche in questa di disposizione, similarmente a quanto rilevato in sede di analisi delle disposizioni relative al titolare e al responsabile del trattamento, è ribadito il generale obbligo in capo a tali soggetti di mettere «*in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio*». Si configura, ancora una volta, quell'obbligo tecnico-organizzativo, preliminare all'esecuzione del trattamento, sempre in quell'ottica di efficiente tutela preventiva, che per il legislatore è requisito fondamentale per la correttezza del trattamento stesso. Tale obbligo è regolato prevalentemente dalla considerazione di alcuni requisiti tutti inerenti al trattamento come:

a) lo stato dell'arte;
b) i costi d'attuazione;

c) la natura, l'oggetto, il contesto e la finalità del trattamento; e infine
d) il rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

Dunque questi sono i parametri variabili che la gamma dei soggetti responsabili dell'esecuzione del trattamento devono attentamente sondare prima di poter dare inizio al procedimento stesso, in modo tale di minimizzare, se non eliminare del tutto, i rischi connessi all'attività di trattamento.

I rischi connessi alla mancata previsione di un adeguato sistema di misure di sicurezza, sono quelli riconducibili alla definizione di *data breach*[138], riportata dal Regolamento 679/2016 all'articolo 4 n. 12, e che descrive una violazione dei dati personali come «*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*.».

La "breccia" nel sistema di sicurezza, secondo il dettato normativo, può avvenire illecitamente o accidentalmente, di conseguenza la violazione può conseguire direttamente dall'attività umana, sia essa illecita poiché avente carattere palesemente di dolosa o colposa come ad esempio a causa di gravi negligenze da parte degli operatori, ovvero a seguito di eventi non facilmente prevedibili come ad esempio calamità naturali.

Secondo quanto riportato periodicamente dai principali gestori di reti di comunicazione elettronica i c.d. *security incidents,* consistenti prevalentemente nell'accesso e trasferimento di dati non autorizzato, negli ultimi cinque anni sono in netto aumento e sono capaci altresì di colpire vari settori dell'attività umana[139].

---

[138] Cfr. considerando n. 85 Reg. "*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata."*

[139] S. VIGLIAR, *Data breach e sicurezza informatica,* Cap. XII, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 241 ss. L'autore fa riferimento direttamente al rapporto stilato dal *broadband provider Verizon*, che nel solo 2015 ha

Nello specifico sono stati individuate nove tecniche di attacco e/o modalità mediante il quale può verificarsi un incidente di sicurezza, di cui riporto l'estratto integralmente: «

1) ***Attacchi per mezzo di applicazioni on-line****: si fa riferimento ad ogni incidente ad opera di un malware, cioè da un'applicazione o un software progettati ai fini di abuso, ad esempio per manomettere codici o meccanismi di autenticazione. Tali attacchi si registrano nei settori finanziari o dell'acquisto di beni di consumo, colpendo le informazioni rilasciate da utenti all'atto dell'accesso, della navigazione e dell'interazione all'interno delle pagine di offerta di beni e servizi;*
2) ***Intrusioni nei punti-vendita****: la violazione avviene in relazione agli accessi non autorizzati a dati e informazioni rilasciati all'atto dei pagamenti elettronici, presso alberghi, ristoranti, negozi;*
3) ***Utilizzo abusivo di informazioni riservate****: ogni violazione dei dati che riguarda flussi interni o riservati di informazioni trasmesse attraverso l'accesso a reti interne o aziendali (LAN);*
4) ***Errore****: ogni tipo di azione non intenzionale che pone a repentaglio la sicurezza di un insieme di dati, ad eccezione dello smarrimento di dispositivi;*
5) ***Furto e perdita****: ogni incidente avente ad oggetto beni tangibili che implichi la scomparsa di un insieme di informazioni ascrivibile a smarrimento o a condotte intenzionali;*
6) ***Crimeware****: violazioni causate da un malware che non rientrano nelle classificazioni precedenti. Tali incidenti si registrano prevalentemente nel settore del consumo e sono motivate da interessi di carattere finanziario di gruppi criminali organizzati che operano a livello transnazionale;*
7) ***Skimming****: fattispecie che comporta l'installazione fisica di apparecchi per la captazione fraudolenta di dati, idonei ad alterare il funzionamento*

---

accertato ben 64.199 incidenti, di cui 2.260 sono risultati veri e propri data breach. A tal proposito si rimanda a VERIZON, *2016 Data breach Investigation Report*, 2016.

di dispositivi di lettura di carte magnetiche o dispositivi di pagamento (ad es., prelievi di denaro presso gli sportelli bancari);

8) ***Spionaggio informatico****: atti di spionaggio svolti da enti paragovernativi o relativi ad attività di carattere industriale o manifatturiero;*
9) ***Interruzione del servizio****: qualunque attacco che abbia ad oggetto la compromissione o la disponibilità assoluta, per un intervallo più o meno lungo, di una rete di comunicazione elettronica*.»

È di facile intuizione la portata estremamente dannosa che violazioni di questo genere possono arrecare ai dati personali dei soggetti di volta in volta colpiti. Questo fa sì che per poter efficacemente contrastare veri e propri attacchi ai dati personali degli individui sottoposti a trattamento, siano predisposti adeguati sistemi di difesa, capaci di assicurare un elevato livello di protezione.

A tal proposito sempre il paragrafo 1 dell'articolo 32 predispone un elenco a titolo esemplificativo di misure capaci di alzare il livello di sicurezza[140] e alle quali il titolare e il responsabile del trattamento dovrebbe ricorrere come ad esempio:

a) La pseudonimizzazione e la cifratura dei dati personali;
b) La capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento (garantire di conseguenza l'efficacia costante dei sistemi di sicurezza

[140] Come suggerito in tema di pseudonimizzazione dal considerando n. 28 "*L'applicazione della pseudonimizzazione ai dati personali può ridurre i rischi per gli interessati e aiutare i titolari del trattamento e i responsabili del trattamento a rispettare i loro obblighi di protezione dei dati. L'introduzione esplicita della «pseudonimizzazione» nel presente regolamento non è quindi intesa a precludere altre misure di protezione dei dati."* e dal considerando n. 29 *"Al fine di creare incentivi per l'applicazione della pseudonimizzazione nel trattamento dei dati personali, dovrebbero essere possibili misure di pseudonimizzazione con possibilità di analisi generale all'interno dello stesso titolare del trattamento, qualora il titolare del trattamento abbia adottato le misure tecniche e organizzative necessarie ad assicurare, per il trattamento interessato, l'attuazione del presente regolamento, e che le informazioni aggiuntive per l'attribuzione dei dati personali a un interessato specifico siano conservate separatamente. Il titolare del trattamento che effettua il trattamento dei dati personali dovrebbe indicare le persone autorizzate all'interno dello stesso titolare del trattamento.".* E ancora in tema di cifratura il considerando n. 83 "*per mantenere la sicurezza e prevenire trattamenti in violazione al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura*.".

preposti al trattamento al fine di minimizzare o evitare la possbili verificazione di incidenti fisici e tecnici);

c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (inteso come monitoraggio, verifica periodica e se necessario di aggiornamento delle misure di sicurezza).

La pseudonimizzazione è uno strumento che più volte è portato ad esempio dal legislatore europeo all'interno del Regolamento in varie disposizioni, come valida tecnica di sicurezza avente la capacità di non rendere più riconducibile un dato ad una determinata persona e consentirne di conseguenza un utilizzo che non violi la *privacy* del soggetto a cui i dati prima si riferivano.

Come detto anche in precedenza la pseudonimizzazione è cosa ben diversa dalla tecnica di anonimizzazione dei dati: infatti il dato divenuto anonimo non è da considerare più un dato personale e in quanto tale non è soggetto alla disciplina del Regolamento, poiché in base ai mezzi a disposizione e ai relativi costi che la procedura di de-anonimizzazione comporta, è altamente difficile identificare la persona interessa; al contrario il dato pseudoanonimizzato è in linea generale un dato che è sempre trattato in forma anonima, ma secondo modalità che, ove si renda necessario, rendono facile la identificazione della persona al quale esso si riferisce[141].

Più propriamente per pseudonimizzazione, secondo la definizione predisposta dall'articolo 4 n. 5 del Regolamento UE 2016/679, si intende «*il trattamento dei dati personali in modo tale che i dati personali 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*

[141] In termini pressoché testuali F. PIZZETTI, *PRIVACY E IL DIRITTO EUROPEO ALLA PROTEZIONE DEI DATI PERSONALI*, cit. p. 257.

soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile».

La pseudonimizzazione dunque consiste in un "camuffamento" del dato che, tramite la sostituzione di uno o più attributi con altri (solitamente un attributo univoco), riduce notevolmente la capacità del dato, così mascherato, di essere collegato o collegabile direttamente all'identità di un soggetto. La pseudonimizzazione in ogni caso però non elimina del tutto tale possibilità, non essendo un metodo di anonimizzazione in senso stretto (che riduce pressoché a zero la capacità di collegamento del dato, considerato addirittura non più un dato personale), infatti anche essendo una misura molto utile, la persona fisica potrebbe essere ancora identificata indirettamente, per mezzo del *matching* con ulteriori informazioni.

Come abilmente esplicato dal Gruppo di Lavoro ex art. 29, nel Parere 05/2014 "*Sulle tecniche di anonimizzazione*" (WP216), tanto la tecnica di anonimizzazione quanto la tecnica di pseudonimizzazione incorrono in tre ordini di rischi[142] a seguito dell'applicazione del rispettivo procedimento sul dato e cioè:

a) *Il rischio di individuazione:* che corrisponde alla possibilità di isolare alcuni o tutti i dati che identificano una persona all'interno dell'insieme di dati;
b) *Il rischio di correlabilità:* vale a dire 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). Se un intruso riesce a determinare (ad esempio mediante un'analisi della correlazione) che due dati sono assegnati allo stesso gruppo di persone, ma non è in grado di identificare alcuna persona del gruppo, la tecnica fornisce una protezione contro l'individuazione, ma non contro la correlabilità;

[142] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 "*sulle tecniche di anonimizzazione*" (WP 216), 10 aprile 2014, p. 12.

c) *Il rischio di 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.

Tanto più sono scongiurati tali rischi tanto più risulterà efficiente la misura di sicurezza, anche se lo stesso Gruppo ammette che le tecniche di de-identificazione e di anonimizzazione sono oggetto di ricerca continua e che tale ricerca ha ripetutamente dimostrato che nessuna tecnica è di per sé esente da carenze. Ad ogni modo quanto più vicino allo zero sarà il coefficiente di rischio, tanto più complicato sicuramente sarà per un agente esterno risalire all'identità del soggetto a cui appartiene o apparteneva il dato in origine.

Il Gruppo prosegue elencando poi le tecniche comunemente adoperate per attuare la pseudonimizzazione di un dato tra cui:

a) *crittografia con chiave segreta*, dove solamente chi conosce la chiave può facilmente risalire all'identificazione di ogni persona interessata decrittando l'insieme di dati. Ipotizzando di applicare un sistema di crittografia avanzato, la decrittazione può avvenire solamente se si è a conoscenza della chiave;

b) *funzione di hash*[143], corrisponde a una funzione che, a partire da un'immissione di dati di qualsiasi dimensione, restituisce comunque un'emissione di dimensione fissa; tale funzione non può essere invertita, vale a dire che non esiste più il rischio di inversione associato alla crittografia. Tuttavia, se l'intervallo di valori di immissione relativi alla funzione di hash è noto, la funzione stessa consente di riprodurli al fine di

[143] In informatica una funzione crittografica di hash è un algoritmo matematico che trasforma dei dati di lunghezza arbitraria (*messaggio*) in una stringa binaria di dimensione fissa chiamata *valore di hash*, *impronta del messaggio* o *somma di controllo*, ma spesso anche con il termine inglese *message digest*. Gli algoritmi usati a questo proposito sono unidirezionali (*one-way*), quindi difficili da invertire, questo permette alle funzioni crittografiche di hash di trovare ampio utilizzo negli ambiti di sicurezza informatica come: nelle firme digitali, autenticazione dei messaggi oppure come per la crittografia delle credenziali private degli utenti nelle applicazioni web.
La funzione crittografica di hash ideale deve avere tre proprietà fondamentali: 1) deve essere estremamente semplice calcolare un hash da qualunque tipo di dato; 2) deve essere estremamente difficile o quasi impossibile risalire al testo che ha portato ad un dato hash; 3)deve essere estremamente improbabile che due messaggi differenti, anche se simili, abbiano lo stesso hash.

desumere il valore corretto associato a un dato specifico (ad esempio, se un insieme di dati è stato pseudonimizzato effettuando l'hashing del numero nazionale di identificazione, lo stesso può essere estrapolato semplicemente effettuando l'hashing di tutti i possibili valori di immissione e raffrontando il risultato con i valori contenuti nell'insieme di dati). Si può ricorrere in alternativa a una *funzione di hash con salt* (che prevede l'aggiunta di un valore casuale, noto come "salt", all'attributo oggetto di hashing) che può ridurre la probabilità di estrapolare il valore di immissione, tuttavia permane la possibilità di calcolare con mezzi ragionevolmente utilizzabili il valore dell'attributo originario che si cela dietro al risultato di una funzione di hash con salt;

c) *funzione di hash cifrato con chiave memorizzata*: corrisponde a una funzione di hash particolare che utilizza una chiave segreta quale immissione aggiuntiva (la differenza rispetto alla funzione di hash con salt è che il salt abitualmente non è segreto). In questo caso un intruso avrebbe molte più difficoltà a riprodurre la funzione senza conoscere la chiave, in quanto il numero di possibilità da vagliare è sufficientemente elevato da risultare impraticabile;

d) *crittografia deterministica o funzione di hash cifrato con cancellazione della chiave:* questa tecnica può essere equiparata alla selezione di un numero casuale quale pseudonimo di ciascun attributo contenuto nell'insieme di dati seguita dalla cancellazione della tabella delle corrispondenze. Tale soluzione consente di ridurre il rischio di correlabilità tra i dati personali contenuti nell'insieme di dati e quelli relativi alla medesima persona presenti in un altro insieme di dati in cui viene utilizzato uno pseudonimo diverso. Se si ricorre a un algoritmo particolarmente avanzato, un intruso ha notevoli difficoltà computazionali a cercare di decriptare o riprodurre la funzione, in quanto dovrebbe provare tutte le chiavi possibili, visto che la chiave non è disponibile;

e) *tokenizzazione*: questa tecnica si applica solitamente (anche se non unicamente) nel settore finanziario per sostituire i numeri delle carte d'identità con valori che presentano un'utilità ridotta per un eventuale intruso. Si tratta di una tecnica derivata dalle precedenti in quanto si basa tipicamente sull'applicazione di un meccanismo di crittografia univoca o sull'assegnazione, tramite una funzione indicizzata, di un numero sequenziale o di un numero generato casualmente che non deriva matematicamente dai dati originali.

Al di là della corretta applicazione di queste complicate tecniche di occultamento degli attributi di un dato riferibile ad una persona fisica, il Gruppo raccomanda caldamente di non incorrere nell'errore comune di ritenere sufficiente eliminare o sostituire uno o più attributi per rendere anonimo un insieme di dati poiché «*la semplice modifica dell'identità non impedisce l'identificazione di una persona interessata se l'insieme di dati continua a contenere quasi-identificatori o se i valori di altri attributi consentono comunque di identificare una persona*», di conseguenza «*Occorre adottare misure supplementari per poter considerare l'insieme di dati effettivamente anonimizzato*»[144].

L'insieme di obblighi tecnico-organizzitivi, a carattere preventivo, costituiti dalla predisposizioni delle misure adeguate atte ad assicurare la sicurezza del trattamento, sono completati dalla previsione di una gamma di obblighi, *ex post*, di notifica e comunicazione, gravanti sul titolare e sul responsabile del trattamento a seguito del verificarsi di una violazione della sicurezza dei dati personali[145].

Tali obblighi consistono rispettivamente nel notificare l'avvenuta violazione dei dati all'autorità di controllo e nella comunicazione della violazione direttamente all'interessato.

---

[144] Cfr. GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 "*sulle tecniche di anonimizzazione*" (WP 216), 10 aprile 2014, p. 21 ss.

[145] Si veda GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 03/2014 "*sulla notifica delle violazioni dei dati personali* (WP213) , 25 marzo 2014, dove il Gruppo analizza una serie di ipotesi molto rischiose secondo cui risulterebbe necessario l'adempimento tempestivo degli obblighi di notificazione e comunicazione.

L’articolo 33 prevede che il titolare e il responsabile del trattamento, salvo che risulti improbabile che la violazione possa comportare un rischio per i diritti e le libertà delle persone fisiche, notifiche senza ingiustificato ritardo (quando possibile nel termine stringente di 72 ore dal momento in cui viene a conoscenza) l’avvenuta violazione, allegando in caso contrario successivamente i motivi del ritardo. Al fine di agevolare il controllo e la verifica dei requisiti in merito alla corretta adozione delle misure di sicurezza del trattamento la notifica deve essere corredata dai seguenti elementi essenziali:

a) descrizione della natura della violazione nonché, ove possibile, delle categorie, del numero approssimativo di interessati in questione, delle categorie e del numero approssimativo di registrazioni dei dati personali;
b) comunicazione del nome, dei dati di contatto del responsabile della protezione dei dati (DPO) o di altro punto di contatto presso cui ottenere più informazioni;
c) descrizione delle probabili conseguenze che possono derivare dalla violazione dei dati personali;
d) descrizione delle misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio o per attenuare i possibili effetti negativi della violazione dei dati personali.

In maniera speculare, all’articolo 34, è previsto che, qualora la *data breach* sia suscettibile di comportare un “rischio elevato” per i diritti e le libertà delle persone, il titolare comunichi senza ingiustificato ritardo all’interessato, utilizzando un linguaggio semplice e chiaro (in piena ottemperanza al principio di trasparenza) i dettagli della violazione dei dati personali che lo riguardano, fornendo contemporaneamente le informazioni di cui all’articolo 33, par. 3, lettere b), c) e d).

In caso di inerzia del titolare nell’adempiere agli obblighi di comunicazione presso l’interessato, l’autorità di controllo può richiedere, dopo aver sondato la cogente probabilità che il rischio sia reale e si verifichi, che il titolare vi proceda.

Tuttavia al fine di non aggravare in maniera eccessiva la posizione del titolare del trattamento, imponendo a quest'ultimo a forza adempimenti formali troppo rigidi e a volte non necessari, sono previsti al paragrafo 3 dei casi di esenzione dall'obbligo di comunicazione all'interessato. Di conseguenza il titolare potrà non inoltrare la comunicazione alla persona interessata se alternativamente dimostri che ha messo in atto tutte le misure tecniche di sicurezza adeguate e che tali misure fossero state applicate ai dati oggetto della violazione, di guisa da renderli incomprensibili a chi non avesse autorizzazione all'accesso; oppure se dimostri di aver adottato tali misure successivamente e aver così scongiurato il sopraggiungere del rischio elevato per i diritti e le libertà della persona; o infine quando la comunicazione richiederebbe sforzi sproporzionati, ma in tal caso sono previste forme equivalenti di informazione degli interessati come ad esempio una comunicazione pubblica.

È forte il richiamo al principio di *accountability* (responsabilizzazione) in tutto il blocco normativo inerente le misure di sicurezza e più in generale nella disciplina del trattamento. In base a questo principio infatti il titolare è colui che si fa garante della correttezza, della liceità e della trasparenza delle varie fasi del trattamento dei dati, nonché dei vari principi inerenti la qualità dei dati, le finalità ecc...

Nell'ambito di una *data breach* il titolare, in ossequio al principio di responsabilizzazione, deve essere in grado di valutare autonomamente la portata di tale violazione e prontamente decidere di attuare quegl'interventi settoriali tecnici e organizzativi di tipo riparatorio ed eventualmente attivare le procedure di carattere informativo. Non solo in base al medesimo principio incombe sul titolare l'onere di dimostrare, quando gli viene richiesto, la prova della conformità del suo operato alla *best practice* del settore e alla norme regolamentari, costituendo tale esito positivo una prova liberatoria della responsabilità in caso della verificazione dell'evento dannoso.

6. La valutazione d'impatto sulla protezione dei dati e la consultazione preventiva

L'obiettivo del legislatore europeo di alzare l'asticella della protezione dei dati personali compie un ulteriore passo in avanti grazie all'introduzione di due istituti molto importanti, che sottolineano ancor di più l'importanza di una tutela preventiva e di tipo precauzionale piuttosto che successiva-riparatoria. La valutazione d'impatto e la consultazione preventiva configurano una protezione dei dati personali votata alla pragmaticità, in quanto diventa obbligo cogente compiere tali attività al fine di ottemperare ai principi del trattamento, e votata alla dinamicità, in quanto si tratta di adempimenti che, per la loro stessa natura, devono aggiornarsi, ogniqualvolta le operazioni di trattamento si sviluppano[146].
La valutazione d'impatto e la consultazione preventiva, rappresentano due ulteriori corollari del principio generale di trattamento dei dati personali in modo non rischioso e, in tal senso, questi due strumenti risultano essere presupposti procedurali rispetto alla determinazione e all'adozione delle misure tecnico-organizzative di sicurezza del trattamento. Qui risiede senza dubbi uno dei principali aspetti di importanza dei nuovi istituti: con la previsione obbligatoria e l'applicazione costante da parte dei titolari del trattamento, si anticipa la tutela ad un momento anteriore al trattamento dei dati, non si attende una violazione per poter analizzare i punti deboli del trattamento per poi attuare le corrispondenti misure di sicurezza, ma tramite l'analisi del rischio si individuano in anticipo i rischi verificabili, in base alla tipologia di dati e di operazioni da porre in essere, e potendo così predisporre tutte le misure necessarie e adeguate affinché dal trattamento non derivino lesioni gravi ai diritti e alle libertà delle persone fisiche.
Ai sensi dell'articolo 35 del Regolamento, il titolare effettua una valutazione d'impatto prima di procedere al trattamento, qualora una particolare tipologia di

[146] F. PIZZETTI, *PRIVACY E IL DIRITTO EUROPEO ALLA PROTEZIONE DEI DATI PERSONALI*, cit. p. 295.

trattamento presenti un rischio elevato per i diritti e le libertà delle persone fisiche tenuto conto del fatto che all'interno del procedimento si prevedano l'uso di particolari nuove tecnologie e considerati inoltre il contesto, la natura, l'oggetto e le finalità.

È previsto che durante lo svolgimento della valutazione, qualora sia designato dall'organigramma della struttura del titolare, venga coinvolto quale soggetto professionale il responsabile della protezione dati, che svolge funzione di consulente tecnico.

La valutazione d'impatto si configura come tappa fondamentale e imprescindibile di tutte quelle forme molto rischiose di trattamento, tra le quali a titolo esemplificativo l'articolo 35, par. 3, individua la valutazione sistematica e globale di aspetti personali delle persone fisiche tramite trattamenti automatizzati, compresi la profilazione, e sulle quali si fondano decisioni che esplicano effetti giuridici su dette persone; oppure il trattamento su larga scala di categorie di dati personali c.d. sensibili (dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona);e infine la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Inoltre al fine di facilitare il compito del titolare tanto in sede di valutazione quanto nelle fasi successive, le autorità di controllo possono redigere degli elenchi nei quali sono racchiuse ed esplicate le tipologie di trattamenti per cui si rende necessaria, o non necessaria, una valutazione pre-impatto dei rischi.

Per quanto riguarda infine il contenuto essenziale minimo della valutazione, questo è disciplinato al paragrafo 7, che prevede la presenza necessaria di almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Alla disposizione subito successiva è previsto invece che ogniqualvolta la valutazione d'impatto riveli un reale rischio elevato, in assenza di misure adeguate per attenuarne la pericolosità, il titolare prima di procedere al trattamento, debba consultare obbligatoriamente l'autorità di controllo.

Quest'ultima, qualora il trattamento risulti illecito o carente sotto il profilo dell'adeguatezza per la prevenzione del rischio, ha l'onere di fornire un parere scritto entro otto settimane dalla richiesta di consultazione (prorogabile di ulteriori sei settimane, con il rispettivo obbligo di informativa nei confronti del titolare) con la facoltà di esercitare i poteri investigativi, correttivi, autorizzativi e consultivi previsti all'articolo 58 del Regolamento.

Al fine della redazione del parere scritto, il titolare per rendere completo all'autorità di controllo il quadro generale della situazione le comunica:

a) le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;
b) le finalità e i mezzi del trattamento;
c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati ;
d) i dati di contatto del titolare della protezione dei dati;
e) le risultanze della valutazione di impatto di cui all'articolo 35;
f) ogni altra informazione richiesta dall'autorità di controllo.

Infine tanto la valutazione d'impatto quanto l'autorizzazione preventiva subiscono una deroga nel caso in cui gli Stati membri abbiano previsto

un'autonoma base giuridica per delle particolari ipotesi di trattamento come disciplinato dall'articolo 6 lett. c) ed e), cioè quando il trattamento risulti necessario ad adempiere un obbligo legale in capo al titolare o generalmente sia funzionale all'esecuzione di compiti di interesse pubblico.

7. Le tecniche di protezione dei dati *by design & by default*

Sempre in merito all'approccio proposto dal Regolamento UE 2016/679 basato sulla valutazione del rischio, che esplica la sua funzione precauzionale in una fase prodromica al trattamento e che impone al titolare, secondo il principio di responsabilità (*accountability*), la predisposizione di tutte le misure tecniche e organizzative adeguate, un ruolo importante ha rivestito il pluriennale dibattito sulle *privacy enhancing technologies*[147].

È proprio in questo contesto che emergono due delle novità fondamentali predisposte dal Regolamento generale del 2016, e cioè i concetti di *privacy by design and privacy by default*[148].

---

[147] Per *Privacy enhancing technologies (PET)* si intendono quell'insieme di tecnologie di rafforzamento della privacy. Esistono diverse definizioni delle PET nell'ambito della comunità accademica e dei progetti pilota in questo settore. Secondo il progetto PISA finanziato dalla CE, ad esempio, con PET si intende un sistema coerente di misure nel settore delle TCI (Tecnologia dell'informazione e della comunicazione) che tutela la privacy sopprimendo o riducendo i dati personali ovvero evitando un qualunque trattamento non necessario e/o indesiderato dei dati personali, preservando al contempo la funzionalità del sistema di informazione. . La Commissione, nella sua prima relazione sull'attuazione della direttiva relativa alla protezione dei dati, ha affermato che "*l'utilizzo di misure tecnologiche appropriate costituisce un compromesso essenziale agli strumenti giuridici e dovrebbe costituire parte integrante di qualunque sforzo volto a conseguire un livello sufficiente di tutela della privacy* ...". L'uso delle tecnologie PET dovrebbe consentire di contrastare le violazioni di talune norme sulla protezione dei dati o di contribuire al loro rilevamento. A. GUZZO, *Il concetto di privacy enhancing technlogies*, pubb. in Sicurezza informatica e tutela della privacy, 26 febbraio 2009, reperibile all'indirizzo www.diritto.it.

[148] Come sottolineato più volte, all'interno del suo volume, dal prof. Pizzetti i termini privacy e protezione dati sono molto differenti non solo da un punto di vista terminologico, ma anche concettuale e storico. Non a caso il legislatore europeo, prima con la Dir. 95/46, e ora con il Regolamento 2016/679, non usa mai il termine privacy ma bensì il termine *data protection*. Per usare le parole del Pizzetti "*Purtroppo in Italia il termine privacy, forse anche per il nostro inguaribile sciovinismo, continua a campeggiare in tutti i discorsi, e persino sul sito dell'Autorità garante italiana, per scelta fatta dal suo primo Collegio, è www.Garanteprivacy.it. Cosa questa davvero poco razionalmente spiegabile…*" F. PIZZETTI, *Privacy e il diritto europeo…*, cit., in nota p. 287. Si veda sempre ai fini della distinzione terminologica e concettuale tra privacy e protezione dati R. D'ORAZIO, *Protezione dati by default e by design*, Cap. V, in in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 79 ss.

Come anche esplicitato dalla Guida al regolamento predisposta dal Garante della Privacy «*Il Regolamento promuove la responsabilizzazione (accountability) dei titolari del trattamento e l'adozione di approcci e politiche che tengano conto costantemente del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati. Il principio-chiave è «**privacy by design**», ossia garantire la protezione dei dati fin dalla fase di ideazione e progettazione di un trattamento o di un sistema, e adottare comportamenti che consentano di prevenire possibili problematiche.*[149]».

Per *data protection by design and by default* si intendono dei modelli di progettazione prestabiliti secondo formule standard, e conformi ai criteri stabiliti dalla legge, ai quali ogni titolare del trattamento deve adeguarsi affinché il trattamento possa ritenersi lecito.

L'adozione della *protezione by design* fa sì che prima dell'elaborazione di un qualsiasi processo di trattamento dei dati, siano presi in considerazione già dal progetto i profili di riservatezza e di protezione dei dati personali degli interessati, permettendo così di elaborare la strategia organizzativa e tecnica migliore a seconda della tipologia del trattamento, senza dover aspettare il verificarsi di qualche "problema tecnico" perché possano configurarsi le misure di sicurezza pertinenti da applicare.

Infatti la *protection by design* esplica la sua principale funzione nel momento preparatorio e progettuale delle attività di trattamento, dove le misure tecniche e organizzative sono preordinate dal titolare e successivamente vincolate in modo tale da rispettare efficacemente i principi attinenti alla protezione dei dati personali.

Diversamente *la protection by default*, opera in un momento successivo e riguarda nello specifico le modalità e le soluzione tecniche poste in essere dal titolare tramite impostazioni predefinite e corrispondenti ad aspetti tanto quantitativi, quanto qualitativi, della raccolta, della durata della conservazione,

[149] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guida al nuovo regolamento europeo in materia di protezione dati*, in www.garanteprivacy.it, pdf, 2016.

delle finalità del trattamento e dell'accessibilità ai dati in modo tale che la configurazione predeterminata dei sistemi di sicurezza possa garantire che non si verifichino seri danni per le persone coinvolte.

L'articolo 25 intitolato "*Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita*", disciplina rispettivamente al paragrafo 1 la protezione by design, al paragrafo 2 la protezione by default e al paragrafo 3 inserisce come elemento di discolpa a favore del titolare del trattamento l'adozione e la conformità ai meccanismi di certificazione previsti all'articolo 42, par. 1 e 2, del Regolamento.

Per quanto riguarda la protezione fin dalla progettazione si prevede che il titolare del trattamento sia al momento di determinare i mezzi che saranno utilizzati all'interno del procedimento, sia durante il trattamento, pone in essere tutte quelle misure tecniche e organizzative (tra cui si fa specifico riferimento alla pseudonimizzazione) volte ad attuare in modo efficace i principi della protezione dei dati personali. Dunque, al fine di integrare il trattamento con le necessarie garanzie, predisposte dalla normativa regolamentare, e tutelare i diritti dei soggetti interessati, il titolare non può prescindere dal rispetto dei principi fondanti il trattamento: come quello di minimizzazione che prevede che i dati siano «*adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati*»; oppure il principio di finalità del trattamento per cui i dati sono «*raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità*»; o ancora il principio di conservazione dove si prevede che i dati siano «*conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati*»; e infine il principio di integrità e riservatezza per cui i dati devono essere «*trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*».

Al fine della determinazione di tali misure il titolare dovrà comunque valutare con attenzione tutto quell'insieme di variabili costituite dallo stato dell'arte delle tecnologie di volta in volta utilizzate, nonché dei costi di attuazione delle procedure. Allo stesso modo andranno considerati la natura, l'ambito d'applicazione, il contesto, le finalità del trattamento e la probabilità insieme alla gravità dei rischi a cui cono sottoposti i diritti e le libertà delle persone.
Il quadro che si delinea tuttavia non si presenta come delimitato da rigidi limiti d'applicazione invalicabili, poiché i principi della protezione fin dalla progettazione, come visto sono sottoposti a bilanciamenti e valutazioni in base a canoni di ragionevolezza e proporzionalità che richiamano delle modulazioni applicative variabili a seconda della rilevanza che assumono fattori come la natura, le finalità, il contesto del trattamento e i rischi che ne possono derivare[150].
Invece per quanto riguarda la protezione per impostazione predefinita si prevede che il titolare ponga in essere le misure tecniche e organizzative adeguate affinché per impostazione predefinita siano trattati esclusivamente i dati necessari per ogni specifica finalità (ancora una volta forte è il richiamo ai principi di finalità e minimizzazione), scongiurando il pericolo che i dati personali siano accessibili a un numero indefinito di individui, senza un intervento diretto della persona interessata.

8. Trasferimento dei dati personali verso Paesi terzi od Organizzazioni internazionali

Per quanto riguarda il Capo V quello inerente il trasferimento dei dati personali al di fuori del territorio dell'Unione, verso Paesi terzi e Organizzazioni internazionali, il Regolamento UE 2016/679 apporta alcune significative modifiche senza allontanarsi troppo dal tracciato suggerito dalla Direttiva 95/46/CE. Questo specifico settore negli ultimi anni è stato al centro dei riflettori del panorama giuridico mondiale, e non solo, a causa degli sconvolgenti risvolti

[150] Come analizzato da R. D'ORAZIO, *Protezione dati by default e by design*, cit., p. 83 ss.

scaturiti dalle rilevazioni di Edward Snowden e dalla vicenda *Datagate*[151], che portarono inoltre al ricorso del cittadino austriaco Maximillian Schrems[152] che fu la principale causa dell'annullamento degli accordi *Safe Harbor* tra UE-USA, creando non poche tensioni a livello politico internazionale.

Di conseguenza il legislatore europeo del 2016, ha dovuto necessariamente fare tesoro degli orientamenti che si sono succeduti dalla Direttiva Madre in poi e dei profili di debolezza che il settore del trasferimento dei dati, al di fuori del territorio dell'Unione, ha sofferto in questi anni prendendo le necessarie contromisure e stabilendo regole rigide al quale sottoporre le richieste di trasferimento.

Innanzitutto rispetto alla previsione della Direttiva del '95, il Regolamento amplia il campo di applicazione prevedendo il trasferimento non solo verso Paesi terzi, ma anche verso le Organizzazioni internazionali che per i loro scopi si ritrovano a dover trattare dati personali.

Rimane centrale nel Regolamento, come previsto anche dalla Direttiva, il concetto di *adequacy*[153] come requisito essenziale per permettere il trasferimento verso Paesi terzi e Organizzazioni internazionali qualora quest'ultimi «*garantiscono un livello di protezione adeguato*», e la relativa decisione in merito al possesso di tale requisito spetta alla Commissione che redige in tal proposito una decisione.

---

[151] Con il nome *Datagate* si identificano una serie di rivelazioni sulle attività di sorveglianza di massa nei confronti dei cittadini statunitensi e stranieri compiute dall'agenzia statunitense Nsa dal 2001. Le attività sono proseguite almeno fino al 2011. Il caso si è aperto in seguito alla pubblicazione di alcuni documenti riservati diffusi da Edward Snowden, un ex consulente dell'Nsa entrato in possesso dei file mentre lavorava per la Booz Allen Hamilton, un'azienda che collabora con il dipartimento della difesa e i servizi d'intelligence degli Stati Uniti. Per ulteriori delucidazioni sulle informazione rivelate da Edward Snowden, si rimanda ad una descrizione temporalmente scandita al sito www.internazionale.it.

[152] CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), Sentenza nella causa C-362/14 Maximillian Schrems vsData Protection Commissioner, Lussemburgo, 6 ottobre 2015.

[153] Per dirla con le parole del prof. Franco Pizzetti "*proprio questo è il punto di maggior tensione rispetto agli Stati Uniti, che da tempo insistono invece per far valere il diverso, e persino opposto principio della interoperabilità(...) Nella visione USA della privacy si ritiene in linea generale, che ciò che deve essere protetto è soprattutto l'eventuale danno che un trattamento illecito di dati possa produrre, non un astratto diritto fondamentale alla tutela del dato considerato come proprietà dell'interessato*." F. PIZZETTI, *Privacy e il diritto…*, cit., p. 161-162.

Ad ogni modo anche il concetto di *adequacy* risulta avere una maggiore estensione, rispetto all'antenato presente nella Direttiva 95/46, in quanto sono specificati minuziosamente i principi generali che sottostanno alla disciplina del trasferimento (art. 44), i requisiti che un paese terzo deve avere affinché la Commissione possa deliberare in favore della sussistenza dell'adeguatezza della protezione (art. 45, par. 2), e inoltre che il requisito dell'*adequacy* possa essere anche concesso a un territorio o più settori specifici all'interno del paese terzo ampliando decisamente il campo d'applicazione della disciplina.

Di conseguenza, nel valutare l'adeguatezza del livello di protezione la Commissione deve prendere in considerazione specifici elementi elencati ampliamente al paragrafo 2 dell'articolo 45.

Il legislatore comunitario individua tre gruppi di elementi che la Commissione è tenuta a valutare, al fine anche di ridurre la discrezionalità della Commissione a riguardo, come suggerito a livello giurisprudenziale dalla Corte di Giustizia europea nella sentenza Schrems.

Il primo gruppo di elementi raccoglie valutazioni concernenti «*lo Stato di diritto, il rispetto dei diritti umani e delle libertà fondamentali, la pertinente legislazione generale e settoriale (anche in materia di sicurezza pubblica, difesa, sicurezza nazionale, diritto penale e accesso delle autorità pubbliche ai dati personali), così come l'attuazione di tale legislazione, le norme in materia di protezione dei dati, le norme professionali e le misure di sicurezza, comprese le norme per il trasferimento successivo dei dati personali verso un altro paese terzo o un'altra organizzazione internazionale, la giurisprudenza nonché i diritti effettivi e azionabili degli interessati e un ricorso effettivo in sede amministrativa e giudiziaria per gli interessati i cui dati personali sono oggetto di trasferimento*».

Il secondo gruppo di elementi riguarda la verifica da parte della Commissione in merito alla «*l'esistenza e l'effettivo funzionamento di una o più autorità di controllo indipendenti nel paese terzo o cui è soggetta un'organizzazione internazionale, con competenza per garantire e controllare il rispetto delle norme in materia di protezione dei dati, comprensiva di adeguati poteri di*

esecuzione, per assistere e fornire consulenza agli interessati in merito all'esercizio dei loro diritti e cooperare con le autorità di controllo degli Stati membri».

Infine il terzo gruppo di elementi da valutare annovera «*gli impegni internazionali assunti dal paese terzo o dall'organizzazione internazionale in questione o altri obblighi derivanti da convenzioni o strumenti giuridicamente vincolanti come pure dalla loro partecipazione a sistemi multilaterali o regionali, in particolare in relazione alla protezione dei dati personali.*».

Risulta chiara dunque la volontà del legislatore di sottoporre la Commissione ad una attenta valutazione di tipo "prognostico", atta a valutare preliminarmente l'attendibilità del soggetto e valutare la protezione che effettivamente riserva alla protezione dei dati personali.

Inoltre recependo i suggerimenti della Corte di Giustizia nei successivi paragrafi dell'articolo 45, il legislatore predispone dei sistemi di monitoraggio degli sviluppi della situazione del paese terzo in merito alla valutazione previamente concessa, prevedendo una serie di obblighi direttamente in capo alla Commissione: come quando prevede che l'atto di esecuzione sia sottoposto ad un meccanismo di riesame periodico ogni quattro anni, che tenga conto degli sviluppi nei paesi terzi e nelle organizzazioni internazionali che hanno ricevuto il *placet* della Commissione (par. 3); oppure quando non risulti più adeguato il livello di tutela garantito dal paese terzo, la possibilità per la Commissione di revocare, modificare , sospendere l'efficacia dell'accordo mediante atti di esecuzione senza effetto retroattivo (par. 5); o ancora quando a seguito di revoca, modifica, sospensione la Commissione intavola delle consultazioni per porre rimedio alla situazione che è stata causa dell'interruzione del rapporto di scambio (par. 6).

Al paragrafo 8 è previsto che la Commissione pubblichi sulla Gazzetta Ufficiale dell'Unione europea e sul proprio sito web l'elenco dei Paesi terzi, organizzazioni internazionali ecc., suddividendoli rispettivamente tra chi garantisce o meno un livello adeguato di protezione dei dati personali conforme

ai canoni del diritto fondamentale sancito dalla Carta dei diritti fondamentali dell'Unione europea.

Infine al paragrafo 9 con una norma di diritto transitorio il legislatore sancisce l'efficacia delle decisione prese dalla Commissione sulla base dell'articolo 25, par. 6, della direttiva 95/46/CE, fino al momento in cui non saranno modificate, sostituite o revocate da un'ulteriore decisione futura della Commissione secondo quanto previsto ai paragrafi 3 o 5 dell'articolo 45 del nuovo Regolamento.

Come detto in precedenza molte delle novità introdotte nel Regolamento, in tema di trasferimento dei dati personali, sono figlie delle vicende legate allo scoppio dello scandalo *Datagate* a seguito delle rivelazioni di Edward Snowden sul controllo di massa operato da parte dell'agenzia americana NSA (Agenzia per la Sicurezza Nazionale degli Stati Uniti d'America), ma soprattutto a seguito della vicenda giudiziaria che ha visto coinvolto uno studente austriaco, meglio conosciuta come il caso Schrems[154].

La vicenda ebbe inizio dal ricorso proposto all'autorità garante per la protezione dati irlandese nei confronti di Facebook Ireland Ltd, responsabile del trattamento dei dati degli utenti del social network sul territorio dell'Unione, da un cittadino austriaco di nome Maximillian Schrems che lamentava una grave violazione del diritto alla protezione perpetrata tramite il trasferimento dei dati verso gli Stati Uniti. Infatti, i dati raccolti dalle filiali di Facebook sul territorio dei vari paesi dell'Unione europea venivano trasmessi poi ai server della casa madre americana Facebook Inc. per eseguire un ulteriore trattamento (rispetto a quello già applicato dagli Stati membri) sul suolo americano prima di essere successivamente archiviati. Tale trasferimento di dati tra UE e USA avveniva

[154] In merito alla vicenda giudiziaria del caso Schrems si rimanda alle analisi e i commenti di R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europea alla privacy*, in *Giurisprudenza Costituzionale*, Anno LXI Fasc. 1, Milano, 2016; B. CAROTTI, *Il caso Schrems, del conflitto tra riservatezza e sorveglianza di massa – il commento*, in *Giornale Dir. Amm.*, 2016; M. TRESCA, *Sicurezza vs protezione dei dati: la CGUE cambia registro*, in *Amministrazione In Cammino*, 2016; M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: dei diritti" violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 2016; F. ROSSI DAL POZZO, *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbor al Privacy Shield)*, in *Rivista di diritto internazionale*, Milano, 2016.

sulla base della decisione di adeguatezza della Commissione[155] (adottata al tempo ai sensi dell'art. 25 Dir.) con lo scopo di dare esecuzione ad un accordo concluso tra Unione e il Department of Commerce degli Stati Uniti chiamato *Safe Harbor*.
L'accordo in questione aveva importantissimi risvolti sul piano economico poiché si acconsentiva a che moltissimi enti statunitensi di ricevere dati personali provenienti dall'Unione europea, in cambio gli enti americani dovevano impegnarsi al rispetto dei principi stabiliti per la legittimità del trattamento attraverso uno strumento di autocertificazione.
Maximillian Schrems ricorreva, lamentando gravi carenze e inadempimenti rispetto al livello di adeguatezza di tutela garantita dagli Stati Uniti, ponendo in aperta discussione la decisione della Commissione.
L'autorità irlandese contemplata in prima istanza, rigettava il ricorso in quanto non competente a sindacare la validità della decisione di adeguatezza della Commissione, che rappresentava un atto obbligatorio e vincolante ai sensi dell'art. 228 TFUE, e al quale perciò l'autorità di controllo doveva conformarsi.
Successivamente Schrems impugnava il rigetto direttamente davanti alla High Court d'Irlanda, la quale però rilevò la necessità di operare un rinvio pregiudiziale dinanzi alla Corte di Giustizia europea al fine di chiarire se le autorità nazionali di controllo potessero discostarsi direttamente da un decisione di adeguatezza della Commissione, qualora successivamente all'adozione di essa si fosse palesata una sopravvenuta inadeguatezza del livello di protezione da parte del paese terzo.
La Corte di Giustizia in proposito specificò che le autorità garanti nazionali non possono disattendere, sospendere, vietare un trasferimento contrariamente a quanto stabilito da una decisone di adeguatezza della Commissione, per due ordini di motivi:

a) il tenore letterale della direttiva 95/46 depone in tal senso quando afferma che «*Gli Stati membri adottano le misure necessarie per conformarsi alla*

[155] Decisone della Commissione n. 520 del 26 luglio 2000.

decisione della Commissione» in base anche a quanto stabilito dall'art. 288 TFUE;

b) il principio generale del primato del diritto comunitario su quello interno.

Di conseguenza l'unica modalità d'azione che si presenta ai Garanti nazionali è quella di proporre ricorso alle autorità giurisdizionali del proprio Stato membro di appartenenza ai fini di un successivo rinvio pregiudiziale di fronte alla Corte di Giustizia europea.

La CGUE inoltre sottolineò l'esigenza di limitare la discrezionalità della Commissione in merito alla valutazione dell'adeguatezza del sistema di protezione dei dati personali, incanalandola in binari più rigorosi, e inoltre la necessità di prevedere un efficace sistema di monitoraggio periodico, che testasse la sussistenza dei requisiti di adeguatezza in capo ai Paesi terzi.

La Corte esaminati i motivi di ricorso e le preoccupazioni palesate da Schrems accertò l'inadeguatezza del sistema di tutela predisposto dal *Safe Harbor*, e di conseguenza invalidò la decisione della Commissione, sgretolando le fondamenta della base giuridica sulla quale poggiava l'accordo tra UE e USA, generando non poche tensioni nei rapporti tra le due fazioni.

Proseguendo nell'analisi della disciplina del trasferimento dei dati personali al di fuori del territorio dell'Unione di interesse sono le disposizioni ci cui agli articoli 46, 49 e 50 che regolano rispettivamente: il trasferimento soggetto a garanzie adeguate, le deroghe e la cooperazione internazionale.

L'articolo 46 prevede la possibilità di consentire al titolare del trattamento il trasferimento di dati verso soggetti esterni anche in assenza di una decisione di adeguatezza della Commissione, a condizione siano fornite garanzie adeguate e che gli interessati dispongano di diritti azionabili e mezzi di ricorso effettivi.

Tali garanzie si suddividono in due categorie a seconda che sia necessaria o meno l'autorizzazione da parte dell'autorità di controllo.

Costituiscono garanzie adeguate, che non necessitano di previa autorizzazione:

a) gli strumenti giuridicamente vincolanti e aventi efficacia esecutiva tra autorità pubbliche o organismi pubblici;

b) le norme vincolanti d'impresa;
c) le clausole tipo di protezione dei dati adottate dalla Commissione;
d) le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione;
e) un codice di condotta approvato a norma dell'articolo 40 o un meccanismo si certificazione approvato a norma dell'articolo 42,unitamente all'impegno vincolante ed esecutivo da parte del titolare del trattamento o del responsabile del trattamento nel paese terzo ad applicare le garanzie adeguate, anche per quanto riguarda i diritti degli interessati.

Costituiscono garanzie adeguate, ma necessitano di una previa autorizzazione da parte dell'autorità di controllo:

a) le clausole contrattuali tra il titolare del trattamento o il responsabile del trattamento e il titolare del trattamento, il responsabile del trattamento o il destinatario dei dati personali nel paese terzo o nell'organizzazione internazionale;
b) le disposizioni da inserire in accordi amministrativi tra autorità pubbliche o organismi pubblici che comprendono diritti effettivi e azionabili per gli interessati.

Per quanto riguarda il sistema di deroghe non sembrano esserci particolari innovazioni rispetto alla direttiva del '95, salvo la usuale vocazione al dettaglio e alla maggiore completezza possibile, mentre i contenuti sono per lo più sovrapponibili.

Sono individuabili otto deroghe al divieto di trasferimento in mancanza degli strumenti di valutazione che lo consentono, descritti negli articoli precedenti, e cioè quando si verificano una delle seguenti condizioni:

a) l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di dovuti alla mancanza di una decisione di adeguatezza;

b) il trasferimento sia necessario all'esecuzione di un contratto concluso tra l'interessato e il titolare del trattamento ovvero all'esecuzione di misure precontrattuali adottate su istanza dell'interessato;
c) il trasferimento sia necessario per la conclusione o l'esecuzione di un contratto stipulato tra il titolare del trattamento e un'altra persona fisica o giuridica a favore dell'interessato;
d) il trasferimento sia necessario per importanti motivi di interesse pubblico;
e) il trasferimento sia necessario per accertare, esercitare o difendere un diritto in sede giudiziaria;
f) il trasferimento sia necessario per tutelare gli interessi vitali dell'interessato o di altre persone, qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso;
g) il trasferimento sia effettuato a partire da un registro che, a norma del diritto dell'Unione o degli Stati membri, mira a fornire informazioni al pubblico e può esser consultato tanto dal pubblico in generale quanto da chiunque sia in grado di dimostrare un legittimo interesse;
h) il trasferimento verso un paese terzo o un'organizzazione internazionale non sia ripetitivo, riguardi un numero limitato di interessati, sia necessario per il perseguimento degli interessi legittimi cogenti del titolare del trattamento, su cui non prevalgano gli interessi o i diritti e le libertà dell'interessato, e qualora il titolare del trattamento abbia valutato tutte le circostanze relative al trasferimento e sulla base di tale valutazione abbia fornito garanzie adeguate relativamente alla protezione dei dati personali.

Infine un’ultima novità rilevante è contenuta nell’articolo 50 che predispone una serie di norme mirate a rafforzare la cooperazione internazionale mediante il dialogo tra autorità garanti e Commissione da una parte, paesi terzi e organizzazioni internazionali dall’altra. Questi soggetti cooperano tra loro: al fine di sviluppare meccanismi di cooperazione per applicare efficacemente la

legislazione in tema di protezione dati; al fine di incrementare l'assistenza reciproca tramite scambi di notificazioni, informazioni assistenza alle indagini; tramite il coinvolgimento delle parti interessate in discussioni e attività volte a promuovere la cooperazione; e infine per promuovere lo scambio della documentazione, delle legislazioni e della prassi in materia di protezione dei dati personali, compresi i conflitti di giurisdizione con paesi terzi.

9. Il nuovo sistema delle Autorità Garanti

Un settore che è stato enormemente riformato è sicuramente quello riguardante le Autorità di controllo indipendenti (Capo VI Reg.), che presenta notevoli differenze rispetto all'apparato predisposto ad esempio dalla direttiva 95/46, e che vede crescere sempre di più in importanza il ruolo delle Autorità Garanti che rappresentano il fulcro della vigilanza e della corretta applicazione del Regolamento in modo uniforme su tutto il territorio dell'Unione.

Questa fondamentale differenza tra i due sistemi normativi si spiega agevolmente per due ordini di ragioni: una relativa ai soggetti che hanno partecipato all'elaborazione delle due normative; l'altra basata prevalentemente sulla differente forma normativa utilizzata dai due strumenti[156].

Infatti all'epoca dell'emanazione della Direttiva Madre non esistevano le Autorità di controllo o il Gruppo articolo 29, anzi era proprio tramite la direttiva di armonizzazione che per la prima si richiedeva la presenza di un Garante per la protezione dei dati personali sul territorio di ogni Stato membro. Il nuovo Regolamento al contrario ha usufruito preziosamente di tutta l'esperienza tanto giurisprudenziale della CGUE, quanto del lavoro paranormativo delle Autorità nazionali e del Gruppo art. 29 recependo molti degli orientamenti da questi soggetti proposti e trasformandole in disposizioni puntuali all'interno del Regolamento.

[156] Ne fa un'ampia analisi F. PIZZETTI, *Privacy e il diritto europeo…*, cit., p. 165 ss.

Per quanto riguarda il secondo aspetto la ragione è tutta di carattere giuridico e attiene fondamentalmente alla forma dello strumento normativo adottata.
La Direttiva 95/46, essendo una direttiva di armonizzazione, mirava a creare un livello minimo di protezione su tutto il territorio europeo, stabilendo principi comuni della materia, ma lasciando ad ogni Stato membro libera disponibilità in merito all'attuazione. Il Regolamento al contrario è un atto generale e obbligatorio, direttamente applicabile che non prevede margini di operabilità da parte degli Stati membri se non espressamente previsti dalla normativa e, anche in quel caso, l'intervento dei legislatori nazionali per quanto discrezionale possa essere, avrà comunque sempre e solo funzione integrativa delle disposizioni regolamentari. Dunque specialmente con riguardo al ruolo delle Autorità Garanti e del nuovo Comitato europeo per la protezione dei dati personali (in inglese *European Data Protection Board*) che sostituirà il Gruppo articolo 29, il Regolamento prevede che la disciplina a riguardo sia il più possibile specifica, ordinata e completa.
La prima sezione del Capo VI sulle autorità di controllo indipendente è dedicata alle condizioni generali che comprendono le condizioni di indipendenza, la nomina dei membri, le norme sulla istituzione dell'autorità.
In linea generale è dunque previsto che ogni Stato membro disponga di una o più autorità pubbliche indipendenti sul territorio con il compito di sorvegliare l'applicazione del regolamento e tutelare i diritti e le libertà fondamentali degli individui (art. 51).
Ai sensi dell'articolo 52, che prevede le condizioni di indipendenza, è prescritto che le autorità agiscano libere e indipendenti, non dovendo subire alcun tipo di pressioni esterne, dirette o indirette, nell'adempimento dei propri compiti e nell'esercizio dei propri poteri. Per garantire l'indipendenza dell'autorità inoltre si richiede che i membri si astengano da qualunque azione incompatibile con le loro funzioni; che lo Stato membro fornisca all'autorità supporto in termini di risorse umane, tecniche e finanziarie, dei locali e delle infrastrutture necessarie per l'adempimento dei suoi compiti; infine è necessario che ogni membro

possegga le qualifiche, l'esperienza e le competenze adeguate nel settore della protezione dei dati, al fine di espletare al meglio le proprie funzione e di concerto rafforzare il requisito dell'indipendenza.

Nell'ambito della seconda sezione che descrive la competenza, i compiti e i poteri delle Autorità garanti interessanti innovazioni sono rappresentate dalla figura dell'Autorità Capofila e del criterio territoriale per la sua competenza.

Prima però, per quanto riguarda le disposizioni inerenti i compiti e i poteri a disposizione delle Autorità di controllo, il Regolamento con l'intento di disciplinare il più minuziosamente possibile la fattispecie, creando un apparato pressoché completo, costruisce due disposizioni "monumentali", data la lunghezza dei i due articoli. Basti pensare che solo nell'individuazione dei compiti il legislatore utilizza nell'elenco le lettere dalla a) fino alla v).

L'articolo 57 di conseguenza enuclea una serie molto ampia di compiti che spettano ad un'autorità di controllo sul proprio territorio, tra cui rientrano il dovere di: sorvegliare sulla corretta applicazione del regolamento (lett. a), promuovere la conoscenza, la consapevolezza e la comprensione verso il pubblico dei rischi, delle dinamiche e delle garanzie relative alla protezione dei dati personali (lett. b); oppure il compito di svolgere funzione di consulenza per i parlamenti, per i governi o per istituzioni nazionali in merito al tema della protezione dei dati (lett. c), promuovere la consapevolezza dei titolari del trattamento riguardo ai loro obblighi e doveri (lett. d), fornire le informazioni su richiesta degli interessati in merito all'esercizio dei propri diritti (lett. e); o ancora l'autorità di controllo tratta i reclami proposti da un interessato, un organismo, un'organizzazione (lett. f), collabora con le altre autorità mediante scambio di informazioni al fine di rafforzare l'assistenza reciproca (lett. g), adotta le clausole contrattuali tipo ex artt. 28, par.8, e 46, par. 2 (lett. j), offre consulenza e supporto in merito alle attività di valutazione d'impatto e consultazione preventiva (lett. k-l), contribuisce all'attività di comitato (lett. t) e più in generale svolge qualsiasi altro compito legato alla protezione dei dati personali (lett. v).

L’articolo 58 del Regolamento riconosce in capo ad ogni autorità la possibilità di esercitare tre gruppi di poteri.

Il primo gruppo è composto dai poteri di indagine tra cui rientrano:

la facoltà di ingiungere al titolare di fornirgli ogni tipo di informazione, consentirgli l’accesso ai dati e ai locali se necessario allo svolgimento dei suoi compiti, oppure la possibilità di svolgere attività di indagine sotto forma di revisione sulla protezione dei dati, di effettuare riesami delle certificazioni rilasciate e infine di notificare al titolare e al responsabile le presunte violazioni delle disposizioni regolamentari.

Il secondo gruppo invece è costituito da poteri correttivi che si esplicano nella facoltà per l’autorità garante di: rivolgere ammonimenti al titolare o al responsabile del trattamento quando il trattamento possa violare o abbia violato le disposizione del regolamento; ingiungere al titolare di soddisfare le richieste dell’interessato all’esercizio dei propri diritti, di conformare il trattamento, comunicare all’interessato l’avvenuta violazione dei dati personali, di limitare temporaneamente o definitivamente il trattamento, di rettificare o cancellare i dati personali, la sospensione dei flussi di dati verso un destinatario in un paese terzo.

Infine il terzo gruppo prevede poteri autorizzati e consultivi nel caso in cui all’autorità sia richiesto di: fornire consulenza ai titolare secondo la procedura di consultazione preventiva, rilasciare pareri destinati ai parlamenti, ai governi, ad altri organismi e istituzioni nazionali nonché al pubblico su questioni riguardanti la protezione dei dati personali; rilasciare certificazioni e approvarne i criteri, adottare le clausole tipo di protezione dei dati di cui all'articolo 28 e all'articolo 46 o infine approvare le norme vincolanti d'impresa.

In chiusura di disposizione è previsto, al paragrafo 4, il principio generale per cui l’esercizio dei poteri di un’autorità di controllo è soggetto a garanzie adeguate quali la possibilità di un ricorso giurisdizionale effettivo e il giusto processo, mentre, al paragrafo 5, si prevede che ogni Stato membro debba disporre per

legge il potere per l'autorità di controllo d'intentare un'azione giudiziale o stragiudiziale qualora sia violato il Regolamento.

Come detto in precedenza nello scenario predisposto dal Regolamento si inserisce una figura del tutto nuova, rappresentata dalla c.d. Autorità di controllo capofila.

Alla fine dell'individuazione della competenza di tale figura è fondamentale il criterio del c.d. meccanismo *one stop shop* o dello "sportello unico". Questo meccanismo a carattere territoriale opera solo esclusivamente per quanto riguarda i trattamenti di dati transfrontalieri in base a due presupposti: il primo statico, che rileva in base al numero di stabilimenti del titolare, il secondo dinamico in base alle attività di trattamento effettive esercitate al di fuori dei confini nazionali che comportino dei riflessi giuridici sostanziali in capo a soggetti che risiedono in più Stati membri.

Infatti la disposizione di cui all'articolo 56 intitolata "*Competenza dell'autorità di controllo capofila*" dispone che «*l'autorità di controllo dello stabilimento principale o dello stabilimento unico del titolare e del trattamento o responsabile del trattamento è competente ad agire in qualità di autorità di controllo capofila per i trattamenti transfrontalieri effettuati dal suddetto titolare*».

All'Autorità capofila competono compiti di cooperazione con le altre autorità di controllo coinvolte[157] anche se, ai sensi del paragrafo 6, solo la Capofila unicamente riveste il ruolo di interlocutore del titolare e/o del responsabile, in merito al trattamento transfrontaliero.

Le modalità di cooperazione tra Autorità capofila e le altre autorità di controllo sono descritte all'articolo 60 del Regolamento 679/2016 in cui è riportato l'*iter* decisionale da seguire[158].

[157] Le altre autorità di controllo sono coinvolte in quanto interessate per la presenza di filiali del responsabile del trattamento o per il coinvolgimento nelle operazioni di trattamento anche di propri cittadini nonché, da ultimo, per aver ricevuto un reclamo avverso detto operatore. In maniera pressoché testuale D. MULA, *Trasferimento verso paesi terzi*, , Cap. XIV, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 283.

[158] Cfr. considerando n. 125 e n. 126.

È previsto un meccanismo di cooperazione per cui tutte le autorità coinvolte guidate dalla Capofila, congiuntamente possono condurre operazioni di indagine, controllo e accertamento nei confronti del titolare del trattamento al fine di raggiungere un consenso. In tal senso è previsto che l'Autorità capofila comunichi le informazioni sulla questione alle altre autorità senza indugio insieme ad un progetto di decisione.

Successivamente le altre autorità di controllo redigono pareri motivati sulla proposta trasmessa dall'Autorità capofila, pareri che nonostante non abbiano natura vincolante, devono essere presi in dovuta considerazione. Infatti ispirata al principio di leale collaborazione, al fine di cementare la cooperazione e non svilire, rendendo poi ai fini dei conti inutile il supporto delle altre autorità, si ritiene che l'Autorità capofila non possa adottare un parere diverso[159].

Qualora una delle autorità di controllo proponga un'obiezione in merito al progetto di decisione (entro un termine di 4 settimane da quando è stata consultata), qualora la Capofila ritenga l'obiezione pertinente, redige un nuovo progetto da sottoporre al vaglio delle altre autorità entro un termine di due settimane; altrimenti ove non ritenga l'obiezione pertinente o non motivata, sottopone la questione al meccanismo di coerenza previsto all'articolo 63 del Regolamento.

Se nessuna obiezione è presentata, il progetto di decisione della Capofila si intende accettato e vincolante per tutte le autorità che vi hanno partecipato, di conseguenza l'Autorità capofila «*adotta la decisione e la notifica allo stabilimento principale o allo stabilimento unico del titolare del trattamento o responsabile del trattamento, a seconda dei casi, e informa le altre autorità di controllo interessate e il comitato la decisione in questione, compresa una sintesi dei fatti e delle motivazioni pertinenti. L'autorità di controllo cui è stato proposto un reclamo informa il reclamante riguardo alla decisione.*[160]».

[159] D. MULA, *Trasferimento*… cit., p.284.
[160] V. articolo 60, paragrafo 7, Regolamento UE/2016/679.

Infine merita menzionare un'altra importante novità costituita dall'introduzione del Comitato europeo per la protezione dei dati personali, al quale il Regolamento dedica l'intera sezione III, del Capo VI, e che sostituirà il Gruppo di Lavoro Comune articolo 29 introdotto con la Direttiva 95/46/CE.

Anche in questo caso il legislatore non risparmia accuratezza e specificità nel definire nel dettaglio composizione, indipendenza e compiti.

Il Comitato è istituito, a norma dell'articolo 68, quale organismo dell'Unione europea, dotato di personalità giuridica, rappresentato dal proprio presidente e composto dalla figura di vertice di ogni autorità di controllo per ciascun Stato membro e dal garante europeo della protezione dati.

Il Comitato opera in piena indipendenza nell'esecuzione dei suoi compiti e nell'esercizio dei suoi poteri come previsto generalmente per ogni autorità garante indipendente.

All'articolo 70 sono previsti i numerosi compiti del Comitato, il cui obiettivo principale è quello di garantire l'applicazione coerente del Regolamento tramite la pubblicazione di linee guida, raccomandazioni, pareri e migliori prassi, oppure tramite l'esame di propria iniziativa o su richiesta di uno dei suoi membri di qualsiasi questione relativa alla protezione dei dati personali e in merito alla interpretazione e applicazione corretta del Regolamento. Inoltre svolge una funzione di consulenza per la Commissione in merito ai formati e alle procedure per lo scambio di informazioni tra titolari del trattamento e autorità di controllo, oppure per valutare l'adeguatezza del livello di protezione di un Paese terzo o di un'organizzazione internazionale.

Inoltre un compito molto importante del Comitato è rappresentato dall'opera di promozione nell'ambito della cooperazione e dell'assistenza reciproca tra autorità di controllo dove è previsto che il Comitato agevoli e implementi lo scambio di informazioni e prassi, di programmi comuni di formazione e di personale, nonché di conoscenze e documentazione sulla legislazione in tema di protezione dei dati personali tra autorità di controllo europee, ma anche di tutto il mondo.

10. L'inasprimento della responsabilità e del sistema sanzionatorio

Il maggiore cambio di prospettiva adottato dal Regolamento UE 2016/679 è senza dubbio quello di aver incentrato il nuovo sistema interamente sulle figure del *Controller* e del *Processor* e sui profili degli obblighi e dei doveri di quest'ultimi, connessi al rispetto delle norme giuridiche e tecniche del trattamento dei dati personali. La disciplina, dunque, non è più incentrata esclusivamente sui diritti dell'interessato, quali perno fondamentale del diritto alla protezione dati, ma la tutela, in un'ottica dichiaratamente preventiva e di tipo precauzionale, passa necessariamente attraverso un'attenta elaborazione di ogni fase del trattamento dei dati (specialmente delle misure di sicurezza) prima che venga posta in essere. La tutela, inoltre, passa attraverso la definizione puntuale degli obblighi e dei doveri dei principali soggetti che partecipano al procedimento (Titolare e Responsabile), in ossequio al principio di responsabilizzazione previsto all'articolo 5, par. 2 del Regolamento.

Il regime di responsabilità civile elaborato dal Regolamento del 2016, è tutt'altro che agevole per il titolare e il responsabile del trattamento che, a norma dell'articolo 82[161], rispondono per qualsiasi danno materiale o immateriale causato da una violazione del Regolamento seguendo, all'accertamento di tale violazione, il diritto al risarcimento del danno a favore dell'interessato che abbia subito il danno. In questa occasione il Regolamento 679/2016 sembra aver seguito le orme del legislatore italiano che, nell'elaborazione del Codice Italiano della Privacy, aveva optato per l'applicabilità dell'articolo 2050[162] c.c. al titolare

[161] La ripartizione della responsabilità prevista dall'articolo 82, par. 2, segue un modello a cascata per il quale il titolare del trattamento « *risponde per il danno cagionato dal suo trattamento che violi il presente regolamento*» , mentre il responsabile del trattamento «*risponde per il danno causato dal trattamento solo se non ha adempiuto gli obblighi del presente regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento*». Inoltre al fine di garantire il risarcimento effettivo dell'interessato è prevista una responsabilità di tipo solidale ogni qualvolta siano responsabili entrambi i soggetti del danno causato (par. 4). È previsto inoltre la possibilità per il titolare o il responsabile che abbia ripagato per intero il risarcimento del danno, il diritto per tale soggetto di reclamare dagli altri titolare e/o responsabili l'ammontare di quota corrispondente la loro parte di responsabilità (par.5).

[162] Codice Civile, articolo 2050, "Responsabilità per l'esercizio di attività pericolose": «*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei*

del trattamento dei dati personali che, secondo lo schema "dell'attività pericolosa", è tenuto a risarcire i danni causati dall'attività di trattamento dei dati se non prova di aver adottato tutte le misure necessarie e idonee a evitare il danno. Infatti tale clausola d'esonero della responsabilità per il titolare e il responsabile del trattamento è riportata dal Regolamento al paragrafo 3 dell'articolo 82, nella parte in cui prevede appunto che «*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità (…) se dimostra che l'evento dannoso non gli è in alcun modo imputabile*».

Dunque la conformità alla regole e ai dettami del Regolamento da parte del titolare e del responsabile del trattamento permette di evitare, da un lato, il rigoroso regime di responsabilità, che come visto prevede una complicata prova di *compliance* al fine di dimostrare l'adeguatezza dell'azione intrapresa, dall'altro lato, le severe sanzioni previste dal Capo VIII.

Per quanto riguarda l'apparato sanzionatorio non ci sono state rilevanti novità, ma sicuramente il Regolamento, decidendo ancora una volta di valorizzare la pericolosità dell'attività di trattamento e l'importanza in termini di gravità di lesioni a cui posso essere sottoposti i dati personali degli individui, ha optato per un deciso inasprimento del regime sanzionatorio, elencando puntualmente modalità, condizioni e importi di erogazione[163].

Le disposizioni principali in tema sono individuate negli articoli 83 e 84 che disciplinano rispettivamente le "*Condizioni generali per infliggere sanzioni amministrative pecuniarie*" e le altre "*Sanzioni*".

In base all'articolo 83 è l'autorità di controllo competente ad infliggere e a determinare l'ammontare della sanzione amministrativa pecuniaria, purché

---

mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.».

[163] A differenza della Direttiva 95/46/CE che si limitava all'articolo 24 intitolato "*Sanzioni*" a prevedere che «*Gli Stati membri adottano le misure appropriate per garantire la piena applicazione delle disposizioni della presente direttiva e in particolare stabiliscono le sanzioni da applicare in caso di violazione delle disposizioni di attuazione della presente direttiva.*» . Si ricorda in ogni caso che la Direttiva del '95 aveva lo scopo di armonizzazione della disciplina all'interno degli ordinamenti dei diversi Stati Membri attraverso il recepimento di un nucleo condiviso di principi, valori e livelli minimi di tutela. Mentre il Regolamento del 2016, per sua natura (generale, vincolante, direttamente efficace e applicabile), richiede maggiore dettaglio e completezza.

quest'ultima sia in ogni singolo caso effettiva, proporzionata e dissuasiva. Colpisce infatti l'ampio margine di discrezionalità che il legislatore europeo affida all'autorità di controllo nella valutazione del *se* e del *quantum* della sanzione, valutazione che in ogni caso dovrà tenere in considerazione, volta per volta, alcuni elementi come:

a) la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o a finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito;
b) il carattere doloso o colposo della violazione;
c) le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati;
d) il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 e 32;
e) eventuali precedenti violazioni pertinenti commesse dal titolare del trattamento o dal responsabile del trattamento;
f) il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi;
g) le categorie di dati personali interessate dalla violazione;
h) la maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione;
i) qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 58, paragrafo 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti;
j) l'adesione ai codici di condotta approvati ai sensi dell'articolo 40 o ai meccanismi di certificazione approvati ai sensi dell'articolo 42; e

k) eventuali altri fattori aggravanti o attenuanti applicabili alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

È specificato inoltre che tali sanzioni amministrative pecuniarie sono inflitte in aggiunta alle misure di cui all'articolo 58, par. 2, che prevede l'elenco dei poteri delle autorità di controllo (di indagine, correttivi, autorizzativi e consultivi).

Secondo quanto previsto dai paragrafi 4, 5 e 6 dell'articolo 83, sono individuate tre tipologie di violazioni alle quali seguono tre sanzioni amministrative pecuniarie: identiche nelle modalità di erogazione, diverse per quanto riguarda l'ammontare della cifra, in modo tale che, a seconda dell'entità della violazione di specie, la sanzione possa assumere quei caratteri di proporzionalità, effettività e di dissuasione sanciti al paragrafo 1.

Nel caso in cui siano violate le disposizioni riguardanti gli obblighi del titolare a norma degli articoli 8, 11, da 25 a 39, 42 e 43; oppure gli obblighi dell'organismo di certificazione (artt. 42 e 43) o dell'organismo di controllo (art. 41, par. 4), l'autorità di controllo può comminare una sanzione amministrativa pecuniaria ("meno grave") fino a 10.000.000 di euro o, per le imprese, sino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

Le sanzioni "più gravi" sono previste invece, qualora siano violate le disposizioni inerenti i principi di base del trattamento, le condizioni del consenso e i diritti degli interessati; i trasferimenti di dati personali verso paesi terzi o verso un'organizzazione internazionale; qualsiasi obbligo imposto da uno Stato membro a norma del Capo IX del Regolamento (Disposizioni relative a specifiche situazioni di trattamento); oppure a causa dell'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione del flusso di dati dell'autorità di controllo ex art. 58, par. 2.

Per queste violazioni sono previste sanzioni pecuniarie più severe che possono raggiungere un ammontare pari a 20.000.000 di euro e fino al 4% del fatturato mondiale annuo precedente, se superiore, per le imprese.

Il paragrafo 8 dell'articolo 83 stabilisce che, in ogni caso, il potere conferito alle autorità di controllo, nell'ambito dell'applicazione delle sanzioni pecuniarie, deve essere soggetto a garanzie procedurali adeguate e conformi al diritto dell'Unione e degli Stati membri, prevedendo un ricorso giurisdizionale effettivo e la garanzia dell'osservanza dei principi del giusto processo.

Infine, il legislatore europeo nell'articolo 84 decide di lasciare un margine di discrezionalità agli Stati membri, permettendo a quest'ultimi di individuare le altre e ulteriori sanzioni per le violazioni del Regolamento. Un margine di operatività che soffre come unico limite quanto già previsto per le violazioni sanzionate ex art. 83, mentre per le altre violazioni il Regolamento richiede soltanto che siano adottati tutti i provvedimenti necessari per assicurare l'applicazione delle sanzioni e che quest'ultime siano effettive, proporzionate e dissuasive.

Ancora una volta si nota il cambio di prospettiva della disciplina in tema di protezione dei dati personali rispetto alla Direttiva 95/46/CE più orientata, di volta in volta, a tutelare il singolo nei confronti del titolare del trattamento.

Il Regolamento invece mira a sanzionare severamente i trattamenti illeciti, in un'ottica ben più ampia rispetto la dimensione del singolo, protesa ad una protezione globale dei soggetti dai trattamenti illeciti, specialmente nel momento in cui il numero rilevante di dati trattati o la tipologia particolare del procedimento integrino rischi collettivi di rilevante dimensione e portata[164].

[164] A. G. PARISI, *Responsabilità e Sanzioni,* Cap. XV, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 310.

Capitolo III

La protezione dei dati personali nell'ambito della pubblica sicurezza e della giustizia penale e le recenti applicazioni giurisprudenziali

Sezione I

La normativa europea di cooperazione giudiziaria e di polizia dalla Convenzione del Consiglio d'Europa fino alla Direttiva generale UE 2016/680

1. Introduzione: lo sviluppo della cooperazione informativa

L'Unione Europea sin dall'entrata in vigore del Trattato di Maastricht nel 1993 che istituisce l'Unione Europea[165] e dalla firma degli accordi di Schengen nel 1995, fino ai giorni nostri, ha cercato di creare uno spazio europeo condiviso, libero e aperto. Tappa fondamentale per l'attuazione dei principi fondanti dell'Unione[166] e delle quattro libertà di circolazione (persone, merci, servizi e capitali) è rappresentata necessariamente da una stretta cooperazione tra tutti gli Stati Membri.

Di pari passo con la crescita dell'Unione e del Mercato Unico europeo, alle tradizionali categorie delle libertà di circolazione, si è aggiunta quella relativa alla libera circolazione dei dati tra i vari Paesi e le Organizzazioni internazionali. Dati che necessariamente portano con sé il proprio "bagaglio culturale" costituito dal sistema di tutela, così come elaborato nel tempo, e dal suo *status* direttamente

[165] L'Unione Europea nata dal Trattato di Maastricht era progettata ancora nella ormai superata (la struttura in pilastri infatti è stata abolita con il Trattato di Lisbona firmato nel 2007, ma entrato in vigore solo nel 2009) struttura a tre pilastri divisa in:
1) Comunità Europea (CE); 2) Politica estera e di sicurezza comune (PESC); 3) Cooperazione di polizia e la cooperazione giudiziaria in materia penale (GAI).

[166] L'Unione garantisce la libera circolazione di persone, merci, servizi e capitali all'interno del suo territorio attraverso un mercato europeo comune e la cittadinanza dell'Unione europea, promuove la pace, i valori e il benessere dei suoi popoli, lotta contro l'esclusione sociale e la discriminazione, favorisce il progresso scientifico e tecnologico e mira alla stabilità politica, alla crescita economica e alla coesione sociale e territoriale tra gli Stati membri, cercando di attenuare le differenze socio-economiche tra i vari stati membri e incrementarne il benessere socio-economico. *I principi fondatori dell'Unione*, in www.europa.eu.

attribuitogli dalla Carta di Nizza, che ha elevato il diritto alla protezione dei dati personali a diritto fondamentale.

Il libero scambio dei dati assume un ruolo rilevante, non solo dal punto di vista strettamente economico o delle dinamiche commerciali afferenti il Mercato Unico, ma riveste un'importanza significativa anche nell'ambito della circolazione delle informazioni per il contrasto della criminalità transfrontaliera.

Nonostante l'importanza che la condivisione di informazioni riveste al fine di fronteggiare le minacce rappresentate dall'operato della criminalità a livello internazionale, il settore della cooperazione giudiziaria e di polizia è sempre stato ostacolato da istanze indipendentiste da parte degli Stati membri che, da un lato, sono poco disposti a cedere la propria sovranità in ambiti come la sicurezza nazionale e il diritto penale in generale, mentre dall'altro, è palpabile una *lack of confidence* per cui in mancanza di garanzie fondate su valori giuridici condivisi e livelli di tutela adeguati, risulta arduo creare una base solida di fiducia reciproca.

A sostegno di tale tesi, inoltre, c'è la mancanza di una normativa comune, uniforme e vincolante in tale settore a livello UE (come ad esempio l'adozione di un regolamento in materia) a differenza di quanto avvenuto per gli altri pilastri.

Nonostante ciò la tematica di un'efficiente cooperazione nel contesto della pubblica sicurezza e della giustizia penale, in termini di diffusione di dati e informazioni, è sempre stata molto sentita e numerosi sono stati gli interventi normativi al fine di armonizzare il più possibile le legislazioni nazionali, creando uno spazio operativo condiviso.

Un impulso decisivo alla cooperazione informativa, intesa come «*la raccolta, l'archiviazione, il trattamento, l'analisi e lo scambio delle pertinenti informazioni*[167]» è stato dato con il Programma dell'Aia del Consiglio europeo di Bruxelles del 4 e 5 novembre 2004.

Il Programma dell'Aia elabora il c.d. principio di disponibilità che apre frontiere del tutto nuove in un settore che, fino a quel momento, era governato dal

[167] TFUE, articolo 87, paragrafo 2 lettera a), intitolato "*Cooperazione di polizia*".

principio opposto del dominio esclusivo sui dati acquisiti nel corso o in funzione delle investigazioni penali da parte delle autorità statali[168].

Il principio di disponibilità fa sì che si adotti una diversa prospettiva ai fini dell'impulso del *law enforcement* dove ogni Stato membro, anche al fine di proteggere la propria sicurezza nazionale, deve collaborare a garantire in primis la sicurezza dell'Unione, abbattendo le barriere informative costitute dai confini nazionali. Secondo la definizione del principio di disponibilità proposta dal Programma dell'Aia la cooperazione e lo scambio di informazioni deve operare in modo tale che «*in tutta l'Unione, un ufficiale di un servizio di contrasto di uno Stato membro che ha bisogno di informazioni nell'esercizio delle sue funzioni può ottenere tali informazioni da un altro Stato membro, e che il servizio di contrasto nell'altro Stato membro che dispone di tali informazioni è tenuto a trasmettergliele per i fini dichiarati, tenendo conto dei requisiti relativi alle indagini in corso nel suddetto Stato.*[169]».

Volendo riassumere, dunque, un'autorità di contrasto deve poter essere nella condizione di individuare lo Stato membro di riferimento che sia in possesso di informazioni utili ai fini delle indagini o per la prevenzione di serie minacce alla pubblica sicurezza, e richiederne la collaborazione mediante la possibilità di accesso a tali informazioni. Collaborazione che, come specificato dal Programma, può avvenire sia con forme di collaborazione diretta tramite il passaggio di dati tra uno Stato all'altro, sia mediante la costituzione di archivi centrali a livello europeo, consultabili direttamente *on-line* dalle autorità di contrasto nazionali.

Un altro passo in avanti per l'attuazione concreta del principio di disponibilità è stato fatto dal Trattato di Prüm[170], il cui nucleo centrale era costituito dal

---

[168] In termini pressoché testuali P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, Cap. XVI, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 314.

[169] Come descritto al punto 2.1 intitolato "*Miglioramento dello scambio di informazioni*", parte III del PROGRAMMA DELL'AIA del Consiglio europeo, Bruxelles, 4 e 5 novembre 2004.

[170] TRATTATO DI PRÜM siglato dal Regno del Belgio, la Repubblica Federale di Germania, Il Regno di Spagna, la Repubblica Francese, il Granducato di Lussemburgo, il Regno dei Paesi Bassi e la Repubblica d'Austria riguardante " *L'approfondimento della cooperazione transfrontaliera, in particolare al fine di*

rafforzamento della cooperazione transfrontaliera al fine di rendere più efficace possibile la lotta contro gravi fenomeni di criminalità come il terrorismo, le forme di associazione criminale e la migrazione illegale.

Il Trattato di Prüm è stato un veicolo di importanti novità in tema di cooperazione informativa prevedendo, da vero "pioniere" della materia, il trasferimento e la creazione di archivi di categorie di dati innovative come ad esempio quelle appartenenti ai dati genetici (grande attenzione è riservata dal Trattato all'utilizzo del DNA a scopi di indagine), dattiloscopici, automobilistici o relativi ad eventi di rilievo transnazionale.

Uno degli obiettivi del Trattato di Prüm era inoltre quello di «*trasferire le disposizioni del presente trattato nel quadro giuridico dell'Unione europea allo scopo di giungere ad un miglioramento dello scambio di informazioni all'interno di tutta l'Unione europea*». L'acquis comunitario è avvenuto con la trasposizione della disciplina del Trattato all'interno dell'ordinamento UE con la decisione 2008/615/GAI, chiamata appunto decisione di Prüm.

Altre decisioni e provvedimenti normativi hanno contribuito nel tempo ad arricchire il panorama della cooperazione europea in tema di lotta ai reati di criminalità organizzata e terrorismo come ad esempio la decisione 2006/960/GAI relativa alla "*semplificazione dello scambio di informazioni ed intelligence tra le autorità degli Stati membri dell'Unione europea incaricate dell'applicazione della legge*" che prevede come obiettivo il più ampio scambio di dati possibile, specialmente in ottica di prevenzione, oppure al fine di perfezionare i sistemi di trasmissione dei dati e gli archivi centralizzati a livello europeo[171].

---

lottare contro il terrorismo, la criminalità transfrontaliera e la migrazione illegale", Prüm (Germania) il 27 maggio 2005.

[171] Si fa riferimento alle numerose decisioni che a livello europeo hanno contribuito a potenziare il sistema di banche dati centrali europee ai fini del *law enforcement* come ad esempio: la decisione 2007/533/GAI istitutiva del *Sistema informativo Schengen* di seconda generazione (SIS II); la decisione 2008/633/GAI *Sistema di informazione visti* (VIS); decisione 2009/371/GAI e decisione 2009/426/GAI istitutive rispettivamente di *Europol* ed *Eurojust*; decisione 2009/917/GAI sulla riforma del *Sistema informativo doganale* (SID); il regolamento UE n.603/2013 riguardante il *Sistema dattilografico europeo* (EURODAC) e infine il regolamento UE n. 1052/2013 in merito al *Sistema europeo di sorveglianza delle frontiere* (EUROSUR).

Tornando al principio di disponibilità nel settore della cooperazione giudiziaria e in materia penale, uno scambio di informazioni in così larga scala ha creato inevitabilmente delle frizioni con il diritto alla protezione dei dati personali.

La costituzione di molteplici banche dati e la massiccia trasmissione, raccolta e circolazione di informazioni devono essere controbilanciate dall'esigenza di salvaguardare i diritti fondamentali della persona, tra cui nello specifico quello della protezione dati, assicurando misure idonee ad assicurare la protezione dei dati raccolti e scambiati.

Come sostenuto dalla dottrina a riguardo, la protezione in questo senso non soddisfa esclusivamente istanze di libertà aventi carattere individuale e soggettive, ma presenterebbe anche un profilo di tipo oggettivo e pubblicistico in quanto assicurando l'integrità e la genuinità del dato informativo, archiviato e scambiato, si scongiurerebbe il rischio che circolino informazioni erronee e della cui affidabilità si possa dubitare[172].

Ciò risulta fondamentale non solo a garantire la tutela dei diritti delle persone coinvolte, ma è funzionale anche, da un lato, ad evitare di appesantire il lavoro delle autorità di contrasto che, recependo una mole di informazioni erronee, si troverebbero in difficoltà nell'individuare quelle corrette, dall'altro lato, ciò risulta utile al fine di cementare la fiducia nella cooperazione tra gli Stati membri che è la base fondante del principio di disponibilità.

Il tema della cooperazione ai fini di indagine, contrasto e prevenzione di gravi reati è un tema ancora oggi molto sentito, specialmente a causa dell'avanzata di una nuova forma di terrorismo islamico, che potremmo definire l'evoluzione di quella matrice combattente ideologica che fu causa dell'attentato alle Twin Towers, l'11 settembre del 2001.

[172] Così come sostenuto da P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, cit., p. 319; si veda inoltre S. CIAMPI, *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in AA. VV., *Cooperazione informativa*, a cura di F. Peroni - M. Gialuz,Trieste, 2009.

Infatti dal passaggio da Al Qaeda all'Isis (IS o Daesh) anche la filosofia del terrore ha subito importanti cambiamenti[173]: come ad esempio il massiccio uso delle nuove tecnologie come l'Internet e i social media a fini di propaganda e arruolamento in tutto il mondo; la graduale scomparsa del sistema cellulare di collegamento tra i vari gruppi di estremisti e la comparsa sullo scenario di nuove tipologie di terroristi, interni al territorio dell'Unione, la cui aspirazione principale non è più tanto quella di combattere nei territori ad est (come era per l'Afghanistan al tempo di Bin Laden), ma quella di combattere l'Occidente dall'interno. Si fa chiaramente riferimento alla figura dei c.d. *lone wolves* (lupi solitari, che spesso sono cittadini nati e residenti in Europa da generazioni, discendenti da famiglie provenienti da Paesi di religione musulmana) che senza alcun apparente collegamento diretto con il nucleo centrale dell'Isis in Siria, si autoaddestrano con le linee guida facilmente reperibili sul web (che oltre a provvedere all'indottrinamento, insegnano come fabbricare esplosivi, utilizzare e reperire armi, insegnano come comportarsi e le accortezze da utilizzare per non destare sospetti all'interno della comunità) che sono state predisposte dagli esponenti principali del sedicente Stato Islamico. La nuova frontiera del terrorismo di nuova generazione, date le dinamiche d'azione spesso imprevedibili, i contorni sfumati che assume la minaccia della *jihad* sempre meno identificabile in un nemico, instilla una costante instabilità e un senso di perenne allarme nelle società occidentali, specialmente a seguito dei ripetuti attacchi degli ultimi tempi a Parigi[174], a Bruxelles e infine nel recentissimo attentato di Manchester durante un concerto della popstar internazionale, Ariana Grande.

[173] Sul tema dello sviluppo del Terrorismo Islamico e sui risvolti di diritto penale sostanziale e procedurale, specialmente a seguito del D. L. 7/2015 c.d. antiterrorismo, si veda F. FASANI, *Terrorismo Islamico e Diritto Penale*, Milano, 2016.

[174] Si fa chiaramente riferimento agli attentati terroristici al teatro Bataclan, allo Stade de France e a tre ristoranti parigini, alla Strage di Nizza sulla Promenade des Anglais, alla sparatoria nella redazione della rivista satirica Charlie Hebdo e alla successiva fuga in Belgio dell'unico attentatore sopravvissuto alla strage del Bataclan, Salah Abdeslam che tanto sconcerto e preoccupazione ha destato nei giorni successivi.

È in questo momento storico, dunque, che si sente ancora più forte l'esigenza di migliorare, intensificare e rendere più agile la circolazione di informazioni e dati tra le autorità nazionali di contrasto, le agenzie dell'Unione e i Paesi terzi senza lasciare che la paura e l'allarme sociale comportino un ingiustificabile restrizione e/o annullamento dei diritti fondamentali della persona, autentici capisaldi di una società democratica.

2. La normativa del Consiglio d'Europa: la Convenzione n. 108/1981 e la Raccomandazione R (87) 15

A livello sopranazionale una delle prime e più importanti normative settoriali sulla protezione dei dati personali è stata rappresentata dalla Convenzione n. 108/1981 del Consiglio d'Europa, adottata a Strasburgo il 28 gennaio del 1981. Infatti nel periodo poco precedente, anche se ancora lontani da un autonomo riconoscimento del diritto alla protezione dei dati personali come un diritto fondamentale, riconoscimento che avverrà solo con la Carta di Nizza e l'opera integrativa del Trattato di Lisbona, già negli ordinamenti nazionali si iniziava a percepire l'importanza di una attenta disciplina in tema di dati personali e dei procedimenti automatizzati di analisi delle informazioni in questione[175]. Dunque la Convenzione n. 108 rappresentò una importante presa di coscienza della necessità di armonizzare, in un settore così delicato, le legislazioni nazionali che contenendo spesso norme di difficile compatibilità reciproca, tendevano di frequente a complicare i rapporti, piuttosto che a favorirli[176].
La Convenzione n. 108 nel suo impianto generale e onnicomprensivo copre tutti i settori della protezione dei dati personali rispetto al trattamento automatizzato, in

[175] Si veda per una scrupolosa analisi storica e delle dinamiche giuridiche dell'evoluzione del diritto alla protezione dei dati personali nel contesto europeo, F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo,* Vol I de *I Diritti nella "rete" della Rete*, Giappichelli, Torino, 2016.
[176] *Ivi* p. 60 ss.

questo modo è racchiuso all'interno del sistema anche il settore di pubblica sicurezza e giustizia penale[177].

Infatti all'articolo 9 della Convenzione è previsto che sia possibile «*derogare alle disposizioni degli articoli 5, 6 e 8* (Qualità dei dati, Categorie speciali di dati, Garanzie supplementari per la persona interessata) *della presente Convenzione quando tale deroga è prevista dalla legge della Parte e costituisce una misura necessaria, in una società democratica: a) per la protezione della sicurezza dello Stato, per la sicurezza pubblica, per gli interessi monetari dello Stato o per la repressione dei reati (...)*».

La Convenzione del Consiglio d'Europa è stata per lungo tempo il centro nevralgico della disciplina della protezione dei dati personali nel settore della cooperazione giudiziaria e di polizia, poiché anche a seguito dell'entrata in vigore della Direttiva Madre nel '95, quest'ultima non estendeva il proprio raggio d'azione normativo su questo specifico settore, secondo quanto previsto dall'esplicita clausola d'esclusione[178] di cui all'articolo articolo 3, paragrafo 2.

Tuttavia il quadro normativo adottato in materia è risultato essere poco idoneo a garantire un adeguato livello di protezione dei diritti individuali a causa soprattutto della carenza di precisione e di dettaglio.

Non a caso il Garante europeo per la protezione dei dati personali[179] più volte ha sottolineato, in vari pareri, l'inadeguatezza d'insieme del sistema.

---

[177] FRA (European Union Agency for Fundamental Rights) – CONSIGLIO D'EUROPA, *Manuale sul diritto europeo in materia di protezione dei dati*, da < www.fra-europa.eu >, pdf, 2014, p.154.

[178] Si ricorda che la Direttiva 95/46/CE nasce in un contesto europeo diverso da quell'odierno, in quanto era ancora presente la suddivisione dell'Unione europea secondo la struttura a tre pilastri. La disciplina era rivolta esclusivamente al primo pilastro da cui ne deriva la clausola d'esclusione di cui all'articolo 3, paragrafo 2 che recita « *Le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali: a) effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario, come quelle previste dai titoli V e VI del trattato sull'Unione europea e comunque ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello Stato in materia di diritto penale (...)*».

[179] Il Garante Europeo per la Protezione dei Dati personali (GEPD), istituito nel 2004 e avente sede in Bruxelles, è l'autorità di vigilanza deputata a garantire che le istituzioni e gli organi dell'UE rispettino il diritto *dei* cittadini al trattamento riservato *dei dati* personali. I compiti principali consistono nel: controllare il trattamento dei dati personali da parte dell'amministrazione dell'UE allo scopo di assicurare il rispetto delle norme sulla privacy, fare da consulente per le istituzioni e gli organi dell'UE su tutti gli aspetti del trattamento dei dati personali e delle relative politiche e legislazioni, gestire le denunce e condurre indagini, collaborare con le amministrazioni nazionali dei paesi dell'UE per assicurare la

Infatti nel terzo parere del GEPD, relativo alla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, l'autorità europea sottolinea come «*gli strumenti esistenti a livello europeo non sono sufficienti. La convenzione 108 del Consiglio d'Europa, vincolante per gli Stati membri, stabilisce i principi fondamentali della protezione dei dati ma, sebbene debba essere interpretata alla luce della giurisprudenza della CEDU, non offre la necessaria precisione (...) La direttiva 95/46, che ha integrato e precisato i principi della convenzione 108 per quanto riguarda il mercato interno, è stata adottata già nel 1995. Tale direttiva non si applica alle attività che rientrano nel terzo pilastro.*[180]».

Concetto che viene ribadito anche nel parere del Garante europeo sul testo di proposta dell'adozione di una decisione di recepimento del Trattato di Prüm[181].

All'interno del novero degli atti del Consiglio d'Europa rientra anche la Raccomandazione adottata dal Comitato dei ministri il 17 settembre 1987 R (87) 15, relativa alla disciplina dell'uso dei dati personali nell'ambito della pubblica sicurezza. Anche in questo caso, però, il Garante europeo per la protezione dei dati personali ha rimarcato come, benché la Raccomandazione non difetti del carattere di precisione richiesta, la natura non vincolante del mezzo utilizzato, non abbia contribuito al rafforzamento del sistema.

In ogni caso la Raccomandazione ha rappresentato un passo molto importante nel settore della cooperazione in materia giudiziaria e di polizia, in quanto introduce principi fondamentali per la protezione dei dati personali regolando la raccolta, la

---

coerenza nell'ambito della protezione dei dati e controllare le nuove tecnologie che possono influire sulla protezione dei dati, in www.europa.eu.

[180] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, relativo alla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, 27 aprile 2007, punto 8.

[181] GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, sull'iniziativa del Regno del Belgio, della Repubblica di Bulgaria, della Repubblica federale di Germania, del Regno di Spagna, della Repubblica francese, del Granducato di Lussemburgo, del Regno dei Paesi Bassi, della Repubblica d'Austria, della Repubblica di Slovenia, della Repubblica slovacca, della Repubblica italiana, della Repubblica di Finlandia, della Repubblica portoghese, della Romania e del Regno di Svezia, in vista dell'adozione di una decisione del Consiglio sul rafforzamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo ed alla criminalità transfrontaliera, 21 luglio 2007, punto 60.

registrazione, l'utilizzo, la comunicazione, le condizioni per il trasferimento, la pubblicità, le modalità di tenuta degli archivi, il diritto d'accesso, di rettifica, di ricorso, la durata della conservazione, l'aggiornamento, le modalità di controllo da parte delle autorità indipendenti e la sicurezza.

La Raccomandazione stigmatizza in maniera decisa la raccolta illimitata e indiscriminata dei dati da parte delle autorità di polizia, limitandola alla sola raccolta dei dati personali necessari per la prevenzione di un pericolo concreto o per la repressione di un reato penale. Si prevede inoltre che ogni ulteriore raccolta di dati debba basarsi su di una legislazione nazionale specifica e che il trattamento dei dati c.d. sensibili siano limitati a quanto assolutamente necessario nel contesto di una particolare indagine[182].

Inoltre in ossequio al principio di esattezza dei dati applicato ai regimi di conservazione, la Raccomandazione prevede che sia operata una chiara distinzione fra i dati amministrativi e quelli detenuti a scopi di polizia, differenziando tra le varie categorie di interessati, sospettati, detenuti, vittime e testimoni, tra fatti reali e quelli basati su sospetti o deduzioni[183].

In aggiunta, è specificato che i dati acquisiti dalla polizia devono essere strettamente limitati per quanto riguarda lo scopo specifico dell'utilizzo al fine della prevenzione e repressione dei reati penali e al mantenimento dell'ordine pubblico, incidendo specialmente per quanto riguarda il trasferimento a terzi.

Il trasferimento di dati in ambito di polizia[184] dovrebbe essere concesso:

a) In base alla presenza di un interesse legittimo alla condivisione delle informazioni;
b) Qualora sussista un chiaro obbligo legale o autorizzazione;
c) A livello internazionale (esclusivamente alle autorità di polizia straniere), se basate su disposizioni giuridiche specifiche come ad esempio accordi

[182] CONSIGLIO D'EUROPA, Comitato dei ministri (1987), Raccomandazione n. R (87) 15, Principio 2 "*Raccolta dei dati*".
[183] *Ibidem*, Principio 3 "*Registrazione dei dati*".
[184] *Ibidem,* Principio 5 "*Comunicazione dei dati*".

internazionali, salvo che non sia necessario a prevenire un pericolo grave e imminente.

È previsto ancora che il trattamento dei dati posto in essere dalle autorità di polizia sia soggetto ad un controllo indipendente esterno, da parte di un'autorità garante, al fine di osservare il rispetto della normativa nazionale[185] in tema di protezione dei dati personali. Infine la Raccomandazione richiede che all'interessato sia riconosciuta tutta la gamma di diritti sanciti dalla Convenzione n. 108, prevedendo anche la possibilità di ricorso presso l'autorità garante in caso di limitazione del diritto d'accesso, nell'interesse di specifiche indagini, ai sensi dell'articolo 9 della Convenzione n. 108/1981[186].

Secondo la giurisprudenza della Corte EDU emerge un costante conflitto tra interesse pubblico e privato che richiede un attento bilanciamento in termini di proporzionalità, laddove interferenze lesive del diritto alla riservatezza (sancito dall'articolo 8 CEDU) sono ammesse esclusivamente nella misura in cui soddisfino *bisogni sociali impellenti*, siano *proporzionate* alle finalità perseguite e si fondino *su ragioni giustificative pertinenti e sufficienti*. Così ad esempio si è pronunciata la Corte EDU nella causa *S. e Marper c. Regno Unito*[187], dove entrambi i ricorrenti erano stati accusati di aver commesso dei reati. Nonostante non fossero stati condannati, i dati relativi le impronte digitali, i profili del DNA e i campioni di cellule appartenenti ai due ricorrenti erano stati conservati e custoditi dalla polizia, in base alla legge che prevedeva la possibilità della conservazione a tempo indeterminato dei dati biometrici delle persone sospettate di aver commesso un reato anche qualora la stessa successivamente venisse assolta o prosciolta. La Corte EDU, nel caso di specie, ha ritenuto la conservazione generale, indiscriminata e illimitata nel tempo di dati personali

[185] *Ibidem*, Principio 1 "*Controllo e notificazione*".
[186] *Ibidem*, Principio 6 "*Pubblicità, diritto di accesso agli archivi di polizia, diritto di rettifica e di ricorso*".
[187] CORTE EUROPEA DEI DIRITTI DELL'UOMO, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008. Si veda anche in tema di bilanciamento tra privacy e interessi pubblici; CORTE EDU, *Klass e altri c. Germania*, n. 5029/71, 6 settembre 1978; CORTE EDU, *Leander c. Svezia*, n. 9248/81, 26 marzo 1987; CORTE EDU, *Allan c. Regno Unito*, n. 48539/99, 5 novembre 2002; CORTE EDU, *Vetter c. Francia*, n. 59842/00, 31 maggio 2005.

un'ingerenza indiscriminata nel diritto al rispetto della vita privata dei ricorrenti in violazione dell'articolo 8 CEDU.

Al contrario nella causa *B. B. c. Francia*, l'ago della bilancia ha pesato sull'interesse pubblico. La Corte in questo caso ha statuito che l'inserimento in una banca dati giudiziaria nazionale, dei dati di una persona condannata per reati sessuali, fosse conforme con l'articolo 8 CEDU, in quanto essendo state attuate garanzie sufficienti per la protezione dei dati, come il diritto dell'interessato di richiedere la cancellazione dei dati, la durata limitata della conservazione e l'accesso limitato agli stessi, non vi era stata una violazione dell'articolo 8 ed era stata rispettato l'equilibrio tra gli interessi in questione.

Nonostante le carenze dei due principali strumenti normativi del Consiglio d'Europa, la Convenzione n. 108 e la Raccomandazione R (87) 15, poiché la prima mancava della necessaria precisione, mentre la seconda era sprovvista di carattere vincolante, l'operato della CEDU è riuscito a ponderare gli interessi in gioco e risolvere adeguatamente il conflitto "naturale" tra le esigenze pubbliche e quelle private, benché rivolto più alla tutela della riservatezza piuttosto che ad un'autentica protezione dei dati personali.

3. La normativa dell'Unione Europea: dalla Decisione quadro 2008/977/GAI alla Direttiva generale UE 2016/680

Per quanto riguarda la normativa di riferimento dell'Unione europea, quest'ultima presenta sicuramente profili di maggiore completezza e precisione, un sistema di principi più ordinati e uniformi, poiché comunque tutti riconducibili al *common core* predisposto dalla Direttiva 95/46/CE.

Benché la Direttiva Madre in modo esplicito escluda dal campo d'applicazione proprio il settore della pubblica sicurezza e della giustizia penale e comunque i «*trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato (compreso il benessere economico dello Stato, laddove tali trattamenti siano connessi a questioni di sicurezza dello Stato) e le attività dello*

Stato in materia di diritto penale[188]», molti dei capisaldi enucleati all'interno della Direttiva stessa, sono stati alla base dei provvedimenti normativi successivi, con le dovute eccezioni e deroghe confacenti al settore in questione.

La tanto sperata predisposizione di un quadro generale per la protezione dei dati personali nell'ambito della cooperazione giudiziaria e di polizia è avvenuta solo nel 2008 con l'adozione della Decisione quadro 2008/977/GAI[189].

La Decisione quadro 2008/977/GAI del Consiglio mira a garantire la protezione dei dati personali delle persone fisiche quando tali dati sono trattati ai fini della prevenzione, dell'indagine, dell'accertamento e del perseguimento dei reati o dell'attuazione di sanzioni penali.

Secondo l'articolo 3 della Decisione quadro, ricalcando quanto previsto anche nella Direttiva Madre, «*La presente decisione quadro si applica al trattamento di dati personali, interamente o parzialmente automatizzato, nonché al trattamento non automatizzato di dati personali figuranti o destinati a figurare negli archivi*».

Esulano dall'oggetto della Decisione gli interessi fondamentali della sicurezza nazionale e le specifiche attività di informazione in questo settore[190], occupandosi la normativa, nello specifico, di approntare una tutela adeguata del diritto alla protezione dati nell'ambito della cooperazione transfrontaliera dei dati personali trasmessi o resi disponibili tra Stati membri, tra Stati membri e autorità, sistemi di informazioni comuni europei e competenti autorità nazionali[191].

Sono ripresi nella Decisione quadro, con il preciso intento di allineare il livello della protezione con quello della Direttiva 95/46/CE, svariati principi base della materia come i principi di legalità, proporzionalità e finalità. In base ai suddetti principi i dati personali possono essere raccolti dalle autorità competenti soltanto per finalità specifiche, esplicite e legittime nell'ambito dell'espletamento dei loro

---

188 DIRETTIVA 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**,** articolo 3, paragrafo 2, intitolato "*Campo d'applicazione*".

189 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*",2008.

190 *Ibidem,* articolo 1, paragrafo 4, intitolato "*Oggetto e campo d'applicazione*".

191 *Ibidem,* considerando n. 7.

compiti e il trattamento deve necessariamente essere conforme alle finalità per i quali sono stati raccolti.

Il trattamento dei dati deve essere legale e adeguato, pertinente e non eccessivo rispetto alle finalità per le quali sono stati raccolti. L'uso dei dati per scopi diversi è ammesso solo a condizione che l'ulteriore trattamento non sia incompatibile con le finalità per le quali i dati sono stati raccolti, le autorità competenti siano autorizzate a trattare tali dati e infine, che il trattamento sia necessario e proporzionato a tale altra finalità[192].

A proposito dell'articolo 2 inerente alle "*Definizioni*" la Decisione quadro aggiunge un qualcosa in più rispetto alla Direttiva del '95 nei procedimenti di "blocco" e "caratterizzazione": il primo consiste nel «*contrassegno dei dati personali memorizzati con l'obiettivo di limitarne il trattamento in futuro*», mentre al contrario, la seconda rappresenta un «*contrassegno dei dati personali memorizzati senza l'obiettivo di limitarne il trattamento in futuro*».

La Decisione quadro riporta comunque tutte le garanzie minime della disciplina commutate dalla Direttiva del '95 anche se, nel settore della cooperazione giudiziaria e di polizia, queste garanzie spesso cedono il passo ad esigenze di pubblica sicurezza o comunque di interesse collettivo, specialmente in presenza di gravi e imminenti minacce, ritenute preminenti.

Ecco allora che all'articolo 4 sono previste le procedure di "*Rettifica, cancellazione e blocco*" che prevedono l'obbligo di curare l'esattezza dei dati personali, a garanzia tanto della correttezza dell'operato delle autorità di contrasto quanto degli interessi dei soggetti coinvolti, facendo in modo che i dati personali siano rettificati se inesatti, altrimenti completati o aggiornati. Inoltre, qualora non fossero più necessari per le finalità alla base della precedente raccolta, per poter essere ulteriormente trattati devono essere resi anonimi o al contrario, bisogna procedere alla cancellazione. Nell'eventualità in cui ci siano ragionevoli motivi di ritenere che dalla cancellazione possa derivare la compromissione degli interessi legittimi della persona interessata, i dati personali

[192] *Ibidem,* articolo 3.

non sono cancellati, ma semplicemente bloccati, subordinando però l'utilizzo dei dati personali per il solo scopo che ha impedito la loro cancellazione.

Anche se in un settore molto delicato, dove la disciplina dell'informativa spesso poco si concilia con le dinamiche della prevenzione e repressione dei reati, specialmente quando la riservatezza delle indagini è vitale al fine di non compromettere eventuali operazioni di contrasto, la Decisione quadro riporta agli articoli 15 e 16 la disciplina dell'informativa. Nella prima disposizione è previsto che il destinatario informi, su richiesta, l'autorità competente che ha trasmesso o reso disponibile i dati personali in merito al loro trattamento (art. 15), mentre nella seconda disposizione si prevede la comunicazione alla persona interessata della raccolta o del trattamento di dati personali da parte delle rispettive autorità competenti, modalità che sarà compito degli Stati membri stabilire conformemente alla legislazione nazionale (art. 16). È previsto inoltre, al secondo paragrafo dell'articolo 16, che nella situazione in cui i dati personali siano trasmessi o resi disponibili tra Stati membri, ciascuno Stato membro possa chiedere che lo Stato destinatario non informi la persona interessata senza il consenso preliminare dell'altro Stato membro.

La Decisione quadro 2008/977/GAI riporta tra i diritti dell'interessato il diritto all'accesso (art. 17), i diritti alla rettifica, cancellazione o blocco (art. 18), il diritto alla compensazione (art. 19) e il diritto ad un ricorso giurisdizionale (art. 20). Così facendo l'interessato ha il diritto di ottenere su richiesta, senza costrizione, ritardi o spese eccessive, almeno la conferma da parte del responsabile del trattamento o dell'autorità nazionale di controllo del fatto che i dati che lo riguardano siano stati trasmessi o resi disponibili, informazioni sui destinatari cui sono stati comunicati i dati e sulle categorie di dati comunicati, nonché dell'avvenuta effettuazione delle verifiche necessarie.

In ogni caso è previsto che gli Stati membri possano adottare disposizioni legislative che limitino l'accesso alle informazioni se tale restrizione, tenendo in debito conto gli interessi legittimi della persona interessata, costituisca una misura necessaria e proporzionata:

a) per non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;
b) per non compromettere la prevenzione, l'indagine, l'accertamento o il perseguimento dei reati o per l'esecuzione delle sanzioni penali;
c) per proteggere la sicurezza pubblica;
d) per proteggere la sicurezza dello Stato;
e) per proteggere la persona interessata o i diritti e le libertà altrui.

L'articolo 18 garantisce agli interessati la possibilità di far valere gli obblighi in capo al responsabile del trattamento[193] di rettifica, cancellazione o blocco dei dati personali che gli appartengono, lasciando però agli Stati membri la decisione se permettere agli interessati di opporre i loro diritti direttamente verso il responsabile del trattamento o per il tramite dell'autorità di controllo.

In caso di rifiuto da parte del responsabile del trattamento ad ottemperare alla richiesta dell'interessato, è comunque previsto l'obbligo di comunicazione per iscritto, dove devono essere riportati anche i mezzi previsti dalla legislazione nazionale per presentare reclamo o ricorso.

In ogni caso all'articolo 20 è previsto che, aldilà dei ricorsi amministrativi proponibili prima di ricorrere all'autorità giudiziaria, la persona interessata ha il diritto di proporre un ricorso giurisdizionale in caso di violazione dei diritti garantitole dal diritto nazionale applicabile e dalla Decisione quadro, mentre all'articolo 19 è predisposto il risarcimento del danno subito a seguito di un trattamento illegale o di qualsiasi altro danno cagionato da un atto incompatibile con le disposizioni nazionali adottate conformemente alla Decisione quadro, nei confronti del responsabile del trattamento o da altra autorità competente in base alla legislazione nazionale.

Al fine di garantire l'integrità del trattamento dei dati personali, la Decisione dispone che vengano prese «*misure tecniche e organizzative adeguate per*

[193] Chiaramente la Decisione quadro 2008/977/CE adotta la stessa terminologia della Direttiva 95/46/CE, per cui il soggetto che ad esempio nel Regolamento generale UE 2016/679 è chiamato "titolare" del trattamento, qui è definito "responsabile". In ogni caso si intende il soggetto «*persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti del trattamento di dati personali*».

proteggere i dati personali dalla distruzione accidentale o illegale, dalla perdita accidentale, alterazione, divulgazione o accesso non autorizzati, segnatamente quando il trattamento comporta la trasmissione di dati attraverso una rete o la loro messa a disposizione mediante la concessione di un accesso diretto automatizzato e da qualsiasi altra forma illegittima di trattamento di dati personali, tenendo conto in particolare dei rischi che il trattamento comporta e della natura dei dati da proteggere.» (art. 22).

Le "misure idonee e adeguate" sono funzionali a impedire il verificarsi di determinate situazioni capaci di incidere negativamente tanto sul diritto alla protezione dei dati personali degli interessati, quanto all'integrità e alla riservatezza delle indagini. A tal fine le misure adottate devono essere in grado di:

a) vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento di dati personali (*controllo dell'accesso alle attrezzature*);
b) impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate (*controllo dei supporti di dati*);
c) impedire che i dati siano inseriti senza autorizzazione e che i dati personali memorizzati siano visionati, modificati o cancellati senza autorizzazione (*controllo della memorizzazione*);
d) impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato di dati mediante attrezzature per la trasmissione di dati (*controllo dell'utente*);
e) garantire che le persone autorizzate a usare un sistema di trattamento automatizzato di dati abbiano accesso solo ai dati cui si riferisce la loro autorizzazione d'accesso (*controllo dell'accesso ai dati*);
f) garantire la possibilità di verificare e accertare a quali organismi siano stati o possano essere trasmessi o resi disponibili i dati (*controllo della trasmissione*);

g) garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato dei dati, il momento dell'introduzione e la persona che l'ha effettuata (*controllo dell'introduzione*);
h) impedire che i dati personali possano essere letti, copiati, modificati o cancellati da persone non autorizzate durante i trasferimenti di dati personali o il trasporto di supporti di dati (*controllo del trasporto*);
i) garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati (*recupero*);
j) garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati (*affidabilità*) e che i dati memorizzati non possano essere falsati da un errore di funzionamento del sistema (*autenticità*).

Come ulteriore strumento a garanzia della conformità del trattamento ai principi base della disciplina e della legittimità del trasferimento, è previsto all'articolo 23 la "*Consultazione preliminare*" dove è fatto obbligo agli Stati membri, nel caso di creazione di una nuova tipologia di archivio, di consultare le autorità nazionali di controllo se all'interno di suddetto archivio sono trattati anche dati c.d. sensibili (e cioè quei dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale), oppure il trattamento applicato, in ragione del ricorso a particolari tecnologie, procedure o meccanismi, comporta rischi specifici per i diritti e le libertà fondamentali della persona.

Per quanto riguarda invece la categoria dei dati sensibili (art. 6) e le decisioni individuali automatizzate (art. 7), si percepisce in parte l'inversione di tendenza rispetto alla Direttiva 95/46/CE, connaturale al settore di competenza della decisione quadro relativa al rafforzamento della cooperazione giudiziaria e di polizia. Ciò che nella Direttiva Madre era posto come deroga ai principi generali del divieto di trattamento dei dati sensibili o in merito alle decisioni individuali

automatizzate capaci di recare un pregiudizio grave ai diritti della persona, ora nella Decisione quadro, diventano la regola.

In tal senso, è prescritto che i dati sensibili possono essere trattati nella misura in cui è «*strettamente necessario*» e se la legislazione nazionale prevede adeguate garanzie. Allo stesso modo, una decisione basata unicamente su un trattamento automatizzato di dati, destinati a valutare taluni aspetti della sua personalità, è ammessa «*soltanto se autorizzata da una legge che precisi i provvedimenti atti a salvaguardare gli interessi legittimi della persona interessata*.».

La Decisione quadro 2008/977/GAI prevede poi alcune accortezze in merito alla verifica della qualità dei dati trasmessi (art. 8), all'obbligo di registrazione e documentazione (art. 10), all'ulteriore trattamento dei dati trasmessi (art. 11) e in merito al trasferimento dei dati a terzi (art. 13).

Anzitutto, come condizione preliminare alla trasmissione dei dati, è prevista una verifica preliminare sulla qualità dei dati in modo tale da garantirne l'affidabilità, dovendo le autorità competenti prendere tutte le misure ragionevoli per evitare che siano trasmessi o resi disponibili dati personali inesatti, incompleti o non più aggiornati. Nel caso in cui i dati trasmessi siano inesatti o trasmessi illegalmente il destinatario deve essere avvisato quanto prima, in modo da disporre immediatamente le misure atte alla rettificazione, cancellazione o blocco del dato inesatto.

Al fine di garantire la conformità dell'operato del responsabile ai principi del trattamento dettati dalla Decisione quadro e controllarne agilmente la responsabilità, tutte le trasmissioni sono registrate o documentate «*ai fini della verifica della legalità del trattamento dei dati, dell'autocontrollo e per garantire l'integrità e la sicurezza dei dati.*».

Il sindacato sulla legittimità dei registri e della documentazione spetta all'autorità di controllo competente per la protezione dei dati personali che verifica e accerta che il trattamento sia avvenuto correttamente appurando, inoltre, l'integrità e la sicurezza dei dati.

Per quanto riguarda l'ulteriore trattamento dei dati trasmessi o resi disponibili da un altro Stato membro, il legislatore comunitario del 2008 ha previsto all'articolo 11 un elenco tassativo di ulteriori finalità per cui è ammissibile un ulteriore trattamento, come ad esempio: la prevenzione, l'indagine, l'accertamento o il perseguimento dei reati o l'esecuzione delle sanzioni penali diversi da quelli per cui i dati sono stati trasmessi o resi disponibili o delle altre procedure giudiziarie e amministrative direttamente connesse, la prevenzione di un'immediata e grave minaccia alla sicurezza pubblica o qualsiasi altra finalità se vi è stata precedentemente autorizzazione dello Stato membro che ha trasmesso i dati o con il consenso della persona interessata espresso conformemente alla legislazione nazionale.

L'articolo 13 invece disciplina il trasferimento dei dati trasmessi o resi disponibili dall'autorità competente di un altro Stato membro alle autorità competenti di paesi terzi o a organismi internazionali. La trasmissione è consentita solo se l'autorità ricevente sia responsabile per la prevenzione, l'indagine, l'accertamento o il perseguimento dei reati o per l'esecuzione delle sanzioni penali e la trasmissione sia necessaria per uno di tali scopi, se lo Stato membro presso cui sono stati ottenuti i dati abbia acconsentito al trasferimento[194] e il paese terzo o l'organismo internazionale interessati assicurino un adeguato[195] livello di protezione per il trattamento di dati previsto.

Nella parte finale del testo normativo il legislatore europeo del 2008 chiarisce il rapporto tra la Decisione quadro e gli accordi conclusi con Paesi terzi (art. 26) da una parte, e con gli atti dell'Unione adottati in precedenza (art. 28), dall'altra. È

[194] È prevista una deroga al consenso dello Stato membro ex articolo 13, paragrafo 2 della Decisione quadro 2008/977/GAI, nel caso in cui tale trasferimento «*sia essenziale per la prevenzione di un'immediata e grave minaccia alla sicurezza pubblica e se il consenso preliminare non può essere ottenuto in tempo utile. L'autorità competente a dare il consenso è in ogni caso informata senza indugio.*».

[195] Secondo il paragrafo 4, articolo 13 della Decisione quadro 2008/977/GAI, l'adeguatezza del livello di protezione «*è valutata tenendo conto di tutte le circostanze relative a un'operazione o a un insieme di operazioni di trasferimento dei dati. In particolare sono presi in considerazione la natura dei dati, la finalità e la durata del trattamento previsto, lo Stato d'origine e lo Stato o l'organismo internazionale di destinazione finale dei dati, le norme di diritto, generali o settoriali, vigenti nel paese terzo o nell'organismo internazionale in questione, nonché le regole professionali e le misure di sicurezza che si applicano.*».

comunque prevista la generale convivenza tra la Decisione quadro e gli atti precedenti dell'Unione europea nonché degli accordi internazionali stipulati dagli Stati membri e l'Unione, in un'ottica di coordinamento e integrazione reciproca.

Nonostante l'avvento di un normativa generale tanto attesa, in tema di protezione dei dati personali all'interno del settore della cooperazione giudiziaria e di polizia, quest'ultima non è stata esente da critiche.

Secondo autorevole dottrina infatti il carattere "minimalista" del testo normativo non ha permesso di raggiungere l'obiettivo di predisporre un livello di protezione adeguato o quantomeno di pari livello con quello fornito dalla Direttiva 95/46/CE, rendendo il risultato alquanto insoddisfacente[196]. Nello specifico perché la decisione non prende in considerazione, insieme ai dati trasmessi o resi disponibili tra Stati membri, il trattamento *purely domestic* enunciando solo un «*generico impegno degli Stati membri, che non ha valore superiore ad un "auspicio"*[197]» affinché la circolazione informativa sia facilitata e il grado di protezione interno sia di pari livello con quello della decisione quadro.

La scelta di escludere il trattamento domestico dalla sfera di regolamentazione, ha senz'altro ostato all'armonizzazione delle normative nazionali su aspetti critici in merito alla raccolta dei dati e pregiudicando i diritti individuali, in quanto diversamente riconosciuti nei diversi Stati membri. Non solo, così facendo si è resa più complicata l'attuazione del principio di disponibilità, aumentando nel contempo la complessità della circolazione e insieme contribuendo a non creare un rapporto di fiducia reciproca, fondamentale in un settore come quello disciplinato dalla Decisione quadro.

---

[196] P. TROISI, *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, Cap. XVI, op. cit., p. 325; si veda anche G. TIBERI, *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in AA. VV., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, a cura di G. GRASSO, L. PICOTTI, R. SICURELLA, Giuffrè, Milano, 2011, nella parte in cui sostiene che la direttiva è contraddistinta da numerose lacune e «*rischia di essere uno strumento già vecchio e inadeguato ad affrontare i problemi che emergono dai nuovi metodi di lavoro che si sono ormai imposti nell'attività di contrasto al terrorismo e alla criminalità, alimentati dagli sviluppi tecnologici degli ultimi anni e dalla richiesta sempre maggiore di dati personali per affrontare le nuove sfide.*». Si vedano in proposito anche le critiche mosse dal GARANTE EUROPEO DELLA PROTEZIONE DEI DATI PERSONALI, Parere del 4 aprile 2007, cit. punti 61-73, e il Terzo Parere del 27 aprile 2007, cit., punti 16-19.

[197] P. TROISI, *Ibidem.*

3. 1. Le decisioni del Consiglio dell'Unione Europea: la Decisione di Prüm

Nel tempo il Consiglio dell'Unione europea[198] ha introdotto strumenti giuridici più specifici sulla protezione dei dati nel settore della cooperazione transfrontaliera, come ad esempio le Decisione quadro che ha integrato all'interno del diritto UE il Trattato di Prüm (decisione 2008/615/GAI) oppure le due Decisioni attuative di Europol (2009/371/GAI) e di Eurojust (2002/187/GAI e successive modifiche).

Lo scopo della c.d. Decisione di Prüm[199] è potenziare la cooperazione transfrontaliera tra i paesi dell'Unione europea (UE) in materia penale, soprattutto nella lotta al terrorismo e alla criminalità internazionale al fine di migliorare lo scambio di informazioni fra le autorità responsabili della prevenzione dei reati e delle relative indagini[200].

La decisione abbraccia vari profili e categorie di dati, utili agli scopi enunciati, tra cui:

a) l'accesso automatizzato ai profili DNA, dati dattiloscopici e taluni dati nazionali di immatricolazione dei veicoli;
b) la trasmissione dei dati in relazione a eventi di rilievo;
c) la trasmissione delle informazioni per prevenire reati terroristici; e

---

[198] Il **Consiglio dell'Unione europea**, anche detto Consiglio dei ministri europei, è un organo dell'Unione europea che insieme al Parlamento europeo esercita il potere legislativo. Ha inoltre funzione di bilancio, di definire e implementare la politica estera e di sicurezza comune, è composto da funzionari a livello ministeriale degli Stati membri. Da non confondere con il **Consiglio europeo**, anch'esso organo UE, ma composto dai capi di Stato o di governo degli Stati membri e che ha il compito di definire le priorità e gli orientamenti politici generali dell'Unione; da distinguere ancora dal **Consiglio d'Europa**, che a differenza dei primi due, non fa parte dell'Unione europea, ma è un'organizzazione internazionale il cui scopo principale è quello di è promuovere la democrazia, i diritti umani, l'identità culturale europea e la ricerca di soluzioni ai problemi sociali in Europa.

[199] DECISIONE QUADRO 2008/615/GAI, Consiglio del 23 giugno 2008, sul "*potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera*", 2008.

[200] Per approfondimenti sull'evoluzione della disciplina europea in tema di cooperazione nella lotta a gravi forme di criminalità e al terrorismo si rimanda alla dettagliata analisi di tutti gli strumenti normativi succedutesi nel tempo da parte di M. O'NEILL, *Terrorism and human rights- EU data protection framework*, Cap. IX, in *The Evolving EU Counter-Terrorism Legal Framework*, Routledge research in EU law, Oxford, 2012. Si veda anche FRA (European Union Agency for Fundamental Rights), CONSIGLIO D'EUROPA, *Manuale sul diritto europeo in materia di protezione dei dati*, da < www.fra-europa.eu >, pdf, 2014.

d) altre misure per potenziare la cooperazione di polizia transfrontaliera.

La Decisione di Prüm richiede ai paesi dell'Unione europea l'impegno a creare schedari nazionali di analisi del DNA per le indagini[201]. Il funzionamento di questi schedari fa sì che i dati indicizzati, contenenti la parte non codificante del DNA[202] e un numero di riferimento che non consente l'individuazione diretta della persona interessata, siano messi a disposizione di altri paesi dell'UE per svolgere consultazioni automatizzate. Tali consultazioni vengono effettuate attraverso punti di contatto nazionali tramite il raffronto dei profili DNA, in maniera mirata, cioè caso per caso. Nell'ambito di una consultazione si constata una concordanza, il punto di contatto nazionale che sta effettuando la consultazione riceve i dati indicizzati in maniera automatizzata. Analoga procedura è applicata anche per i dati indicizzati provenienti dai sistemi d'identificazione automatizzati nazionali delle impronte digitali (Capo II, Sezione II "*Dati dattiloscopici*"). Inoltre i punti di contatto possono avere accesso anche a determinati dati nazionali di immatricolazione dei veicoli tramite consultazione automatizzata *on-line*. Le consultazioni possono essere effettuate soltanto con un numero completo di telaio o un numero completo di immatricolazione (Capo II, Sezione III "*Dati di immatricolazione*").

Per quanto riguarda invece la trasmissione dei dati in relazione a eventi di rilievo[203] (ad esempio eventi sportivi o riunioni del Consiglio europeo) i paesi dell'UE si trasmettono dati non personali tramite i loro punti di contatto nazionali, come richiesto ai fini della prevenzione dei reati e del mantenimento dell'ordine e della sicurezza pubblica.

Al contrario i dati personali possono essere trasmessi solo se si presuppone che le persone interessate costituiscano una minaccia per la sicurezza pubblica o se si ritiene probabile che possano commettere reati in occasione di tali eventi. Tuttavia, questi dati possono essere utilizzati solo in relazione all'evento

[201] DECISIONE QUADRO 2008/615/GAI, (Decisione Prüm), Capo II, Sezione I "*Profili DNA*", articolo 2 "*Creazione di schedari nazionali di anali del DNA*".
[202] Per parte non codificante di DNA si intendono quelle regioni cromosomiche che non contengono alcuna espressione genetica.
[203] DECISIONE QUADRO 2008/615/GAI, (Decisione Prüm), Capo III "*Eventi di rilievo*".

specifico in questione e devono essere immediatamente cancellati non appena siano stati utilizzati per lo scopo prefisso e comunque entro un anno.

Diversamente, allo scopo di prevenire i reati di terrorismo[204], ma solo nella misura richiesta dalle condizioni che portano alla presunzione che i reati possano essere commessi e per casi specifici, gli Stati membri possono trasmettere agli altri paesi dell'UE tramite i punti di contatto nazionali i seguenti dati:

a) cognome e nomi;
b) data e luogo di nascita;
c) una descrizione delle circostanze dalle quali deriva la presunzione che verranno commessi dei reati.

Per quanto riguarda nello specifico la disciplina riportata in tema di protezione dei dati[205] la Decisione quadro richiama esplicitamente un livello di conformità, quantomeno equivalente, ai principi previsti dalla Convenzione n. 108/1981 e della disciplina di settore proposta dalla Raccomandazione R (87) 15. Inoltre, specifica che la disciplina prevista dalla Decisione di Prüm non si applica alla parti originarie firmatarie del Trattato di Prüm.

Gli Stati membri devono garantire che i dati personali trattati in base a questa decisione siano protetti dai rispettivi ordinamenti nazionali, che solo le autorità competenti siano autorizzate a trattare dati personali, assicurando l'esattezza, l'attualità e la sicurezza dei dati, mediante l'attuazione o la predisposizione di procedure capaci di rettificare o cancellare i dati inesatti o i dati che sono stati trasmessi e che non sarebbero dovuti essere trasmessi.

Le autorità, gli organi e i tribunali competenti devono adottare misure tecniche e organizzative per proteggere i dati personali contro la distruzione, la perdita, l'accesso non autorizzato, l'alterazione o la divulgazione non autorizzata. Al fine di verificare la liceità del trattamento di dati personali tanto automatizzato, quanto "non automatizzato", è necessaria la predisposizione di un registro nel quale i vari trattamenti siano segnati in ordine cronologico. Le autorità

[204] *Ibidem,* Capo IV "Misure volte a prevenire i reati terroristici".
[205] *Ibidem,* Capo VI "Disposizioni generali relative alla protezione dei dati".

indipendenti di protezione dei dati nei paesi dell'UE sono responsabili del controllo del trattamento dei dati personali.

Rilevante anche qui è il "*principio di finalità*" per cui i dati personali possono essere trattati solo ed esclusivamente per i fini per i quali sono stati trasmessi. Un ulteriore scopo nel trattamento è consentito solo a seguito del consenso dello Stato membro che gestisce lo schedario. Il trattamento dei dati personali da parte dello Stato membro che effettua la consultazione o il raffronto è autorizzato esclusivamente allo scopo di:

a) accertare la concordanza tra i profili DNA o i dati dattiloscopici raffrontati;
b) predisporre e introdurre una domanda di assistenza giudiziaria da parte delle autorità di polizia o giudiziarie conformemente alla legislazione nazionale in caso di concordanza dei dati;
c) effettuare la registrazione cronologica ai fini del controllo dell'ammissibilità della trasmissione.

Se non più necessari per uno degli scopi di cui sopra o se il tempo di archiviazione previsto dalla legislazione nazionale è scaduto, i dati personali devono essere eliminati.

È riconosciuto ad ogni individuo il diritto ad essere informato in merito alla tipologia dei dati, alla loro provenienza, ai destinatari, alle finalità e alla base giuridica del trattamento di dati in relazione alla sua persona. L'interessato ha altresì il diritto di chiedere la rettifica o la cancellazione dei dati inesatti o trattati in modo illecito, avendo in ogni caso la facoltà di presentare ricorso ad un giudice o ad un tribunale indipendente e richiedere il risarcimento dei danni o altre forme di riparazione giuridica.

3. 2. Le Decisioni del Consiglio dell'Unione Europea: le Decisioni Europol ed Eurojust

Le due agenzie europee Europol ed Eurojust, entrambe con sede all'Aia, sono state istituite rispettivamente dalla Convenzione Europol del 1 ottobre 1998 e dalla Decisione quadro del Consiglio dell'Unione europea n. 187/2002 che ne disciplinano composizione, funzioni e per quel che riguarda specificamente la protezione dei dati personali, il regime di disciplina in merito alla raccolta, al trattamento e alla conservazione in *database* centrali dei dati utili al fine di avvantaggiare e rafforzare la cooperazione in materia giudiziaria e di polizia tra gli Stati membri[206].

Il compito principale di Europol è quello di coordinare, supportare e cooperare con gli Stati membri nelle attività delle forze di polizia al fine di contrasto e prevenzione di gravi crimini transfrontalieri, atti di terrorismo e altre forme di criminalità che coinvolgono due o più Paesi dell'Unione europea.

Tra gli importanti compiti affidati a Europol compaiono attività quali:

a) la raccolta, la conservazione, il trattamento, l'analisi e lo scambio di informazioni;
b) la comunicazione ai paesi dell'UE d'ogni collegamento constatato tra i reati che li riguardano;
c) sostenere i paesi dell'UE nelle indagini e fornire intelligence e supporto analitico;
d) coordinare, organizzare e svolgere indagini e operazioni per sostenere o rafforzare le azioni delle autorità di contrasto dei paesi dell'UE;
e) chiedere ai paesi dell'UE di avviare, svolgere o coordinare indagini in casi specifici e proporre l'istituzione di squadre investigative comuni;
f) sostenere i paesi dell'UE nella prevenzione e nella lotta contro forme di criminalità che sono facilitate, promosse o commesse attraverso Internet;

[206] Cfr. M. O'NEILL, *The Evolving EU Counter-Terrorism Legal Framework*, op. cit., Oxford, 2012 e FRA (European Union Agency for Fundamental Rights), CONSIGLIO D'EUROPA, *Manuale sul diritto europeo in materia di protezione dei dati*, da < www.fra-europa.eu >, pdf, 2014.

g) redigere valutazioni sulle minacce e altri rapporti.

Dunque la funzione di Europol è per lo più di sostegno e di coordinamento, integrando e fornendo supporto con la propria attività alle indagini di competenza degli Stati membri.

Istituto fondamentale previsto dalla Decisione Europol è quello delle unità nazionali previste all'articolo 8.

Le UNE (Unità Nazionali Europol) rappresentano l'unico organo di collegamento tra Europol e le autorità nazionali competenti. Le unità nazionali pongono in essere un rapporto dinamico con Europol con il quale vi è uno scambio di informazioni e intelligence costante, di cui le UNE hanno in cura l'aggiornamento, valutano le informazioni e l'intelligence per conto delle autorità competenti e, successivamente trasmettono loro il relativo materiale, chiedono a Europol consulenza e trasmettono a quest'ultimo informazioni da conservare nelle banche dati. A questo proposito Europol istituisce e mantiene il sistema di informazione Europol[207] e gli archivi di lavoro a scopo di analisi.

Il Sistema di Informazione Europol (SIE)[208] è un database centrale gestito da Europol all'interno del quale confluiscono le informazioni e l'intelligence afferenti alle aree di competenze di Europol, tra cui il terrorismo. Il SIE contiene informazioni in merito a gravi reati internazionali, informazioni su persone sospettate o condannate, strutture e organizzazione di associazioni criminali o terroristiche, dei mezzi e delle modalità d'azione. È un importante sistema di riferimento per gli Stati membri per controllare e comparare informazioni utili su persone o cose d'interesse al fine delle indagini come automobili, numeri di telefono o messaggi e-mail. I dati nel SIE sono memorizzati in differenti "entità"

[207] DECISIONE QUADRO 2009/371/GAI, Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol), articolo 11.

[208] Cfr. EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, Europol Information System (EIS), *A system for information on serious international crimes*, in www.europol.europa.eu. Il Sistema di Informazione Europol non è il solo *database* creato a livello europeo al fine della conservazione e condivisione di informazioni utili tra gli Stati membri. Numerosi sono infatti i sistemi di informazione tra cui: il *Sistema informativo Schengen* (SIS II) di seconda generazione (decisione 2007/533/GAI); il *Sistema di informazione visti* ,VIS (decisione 2008/633/GAI; il *Sistema informativo doganale* (SID) riformato dalla decisione 2009/917/GAI ; il regolamento UE n.603/2013 riguardante il *Sistema dattilografico europeo* (EURODAC) e infine il regolamento UE n. 1052/2013 in merito al *Sistema europeo di sorveglianza delle frontiere* (EUROSUR).

online che possono essere collegate tra loro in modi diversi per creare un quadro strutturato di un caso criminale. Il sistema inoltre consente anche lo stoccaggio e il controllo incrociato automatico di dati biometrici (DNA) e dati relativi a crimini informatici.

Una caratteristica importante del Sistema è rappresentata dal fatto che i dati inseriti rimangono sotto il controllo e sotto la responsabilità dello Stato o dell'autorità che li inserisce nella banca dati, poiché è prevista l'impossibilità che i dati possano essere in qualunque modo alterati da Europol o un altro Stato membro. Il *Data Owner* che inserisce i dati nel sistema deve:

a) garantire la precisione e l'affidabilità dei dati;
b) verificare i limiti di tempo per la memorizzazione dei dati;
c) assicurarsi che i dati siano aggiornati.

Inoltre lo Stato membro che immette i dati nel Sistema definisce le ulteriori restrizioni per gli altri utenti, limitando ad esempio il diritto d'accesso ad alcune informazioni, limitazione che può essere predisposta anche per Europol e le UNE, anche se di norma si prevede in via generale la possibilità per questi soggetti di accedere direttamente a tutti i dati stoccati all'interno della banca dati Europol[209].

L'agenzia europea Eurojust[210] è istituita con Decisione quadro del Consiglio dell'Unione europea 2002/187/GAI[211], il 28 febbraio 2002, con lo specifico intento di rafforzare la lotta contro gravi forme di criminalità, facilitando a livello giudiziario la cooperazione tra gli Stati membri e semplificandone i lavori.

[209] *Ibidem*, Europol Information System, *Security and Data protection*.

[210] Si veda per un'attenta anali del quadro di cooperazione giudiziaria e di polizia in tema di lotta al terrorismo M. O'NEILL, *Terrorism and human rights- EU data protection framework*, Cap. IX, in *The Evolving EU Counter-Terrorism Legal Framework*, Routledge research in EU law, Oxford, 2012. Per un analisi generale si veda FRA (European Union Agency for Fundamental Rights), CONSIGLIO D'EUROPA, *Manuale sul diritto europeo in materia di protezione dei dati*, da www.fra-europa.eu, pdf, 2014

[211] La DECISIONE QUADRO del Consiglio 2002/187/GAI, del 28 febbraio 2002, che istituisce Eurojust per rafforzare la lotta contro le forme gravi di criminalità, ha subito ulteriori modifiche apportate dalla DECISIONE QUADRO 2003/659/GAI, Consiglio del 18 giugno 2003 e dalla DECISIONE QUADRO 2009/426/GAI, Consiglio del 16 dicembre 2008 (decisioni Eurojust).

Così come previsto per l'Europol, anche Eurojust ha personalità giuridica ed è composto da un membro, per ogni Stato, che abbia la qualifica di magistrato del pubblico ministero, di giudice con mandato quadriennale.

Eurojust è competente in materia di indagini e di azioni penali che interessino duo o più Stati membri nelle aeree di criminalità di competenza di Europol allo scopo di facilitare e rendere più efficiente il coordinamento fra le autorità competenti degli Stati membri e agevolare l'esecuzione delle richieste e delle decisioni in materia di cooperazione giudiziaria. Inoltre Eurojust ha il potere di richiedere alle autorità degli Stati membri interessati di avviare indagini o intraprendere azioni penali, istituire squadre investigative comuni (come previsto anche per Europol, con funzione di supporto logistico sul campo) e adottare misure investigative speciali ai fini dell'indagine.

Allo stesso modo di Europol, Eurojust nell'adempiere i propri compiti e nell'esercizio delle proprie funzioni deve essere in grado di poter scambiare informazioni ritenute rilevanti con le autorità competenti, e a tal fine, inevitabilmente pone in essere condotte di trattamento dei dati personali.

Irrinunciabile, secondo la Decisione 2002/187/GAI, è garantire l'applicazione dei principi e le tutele predisposte dalla Convenzione del Consiglio d'Europa n. 108/1981 sulla protezione delle persone rispetto al trattamento automatizzato dei dati personali.

Eurojust può trattare soltanto i dati riguardanti le persone che sono sospettate di avere commesso un reato di competenza dell'Eurojust o che sono state condannate per un siffatto reato, nonché i dati delle vittime e dei testimoni.

Fra le tipologie di dati utilizzabili figurano: l'identità della persona (cognome, nome, data e luogo di nascita, nazionalità, recapiti, professione, numeri di sicurezza sociale, documenti identificativi, profili DNA, fotografie, impronte digitali, ecc.) e la natura dei fatti contestati (qualifica penale, data e luogo in cui sono stati commessi, tipo di indagine, ecc.).

Al fine di un'efficiente raccolta e facilità di gestione dei dati, nonché di trasmissione dei medesimi, Eurojust deve istituire un sistema automatico di

gestione dei fascicoli con archivi di lavoro temporanei e un indice dei dati personali e non personali. I dati personali sono accessibili unicamente ai membri nazionali, ai loro aggiunti e assistenti, alle persone che partecipano ai sistemi di coordinamento nazionali Eurojust, nella misura in cui sono collegate al sistema automatico di gestione dei fascicoli, nonché al personale autorizzato di Eurojust. A tale riguardo, va sottolineato che l'obbligo della riservatezza permane anche dopo la cessazione delle loro funzioni.

Come visto anche per Europol, in seno a Eurojust, un membro del personale è appositamente designato alla protezione dei dati. Il *Data Protection Officer* garantisce la legittimità del trattamento e ha l'obbligo di registrazione per iscritto della trasmissione e ricezione dei dati.

Sono riportate nella Decisione Eurojust tutto l'insieme di diritti a garanzia delle prerogative dell'interessato per cui chiunque ne abbia diritto può consultare i dati personali che lo riguardano e chiederne la rettifica o la cancellazione, qualora siano errati o incompleti. Inoltre chi ritenga di avere riportato un danno imputabile a un trattamento dei dati illecito, ha diritto a presentare una denuncia ai fini del risarcimento del danno. Eurojust è responsabile in conformità al diritto nazionale dello Stato membro in cui ha sede, mentre gli Stati membri sono responsabili a norma della propria legislazione nazionale. La decisione in oggetto fissa limiti all'esercizio de suddetti diritti, ma solo esclusivamente, nel rispetto delle attività di Eurojust, per evitare di compromettere gravemente un'indagine in corso.

Ai sensi del principio di finalità e di conservazione i dati sono utilizzati solo ed esclusivamente per le finalità aderenti all'operato di Eurojust e vengono conservati soltanto per il periodo strettamente necessario alla conclusione delle sue attività.

Eurojust e gli Stati membri sono tenuti a predisporre tutte le misure di sicurezza idonee, adeguate e necessarie ad assicurare la protezione dei dati dalla distruzione, dalla perdita, dalla diffusione, dalla modifica e dall'accesso non autorizzato.

È prevista altresì l'istituzione di un'autorità indipendente di controllo, con il compito di assicurare che il trattamento dei dati personali venga effettuato nel rispetto delle norme stabilite dalla presente Decisione.

3. 3. La Direttiva Generale UE 2016/680: profili di novità ed evoluzione rispetto alla normative precedenti

Più volte si è sottolineato come il quadro normativo d'insieme a livello europeo in tema di cooperazione giudiziaria e di polizia si sia dimostrato lacunoso e frammentato, foriero di inevitabili incomprensioni tanto sul piano interpretativo, quanto sul piano applicativo, tra gli Stati membri.

Un intervento normativo in questo settore, capace di riportare la disciplina sopra un binario di accettabile equilibrio tra privacy e sicurezza, è stata più volte invocato specialmente a causa dell'evoluzione degli elementi fondamentali dell'equazione della cooperazione di giustizia e polizia.

Prima di tutto è cambiata, e si è evoluta, la criminalità e fenomeni come il terrorismo, tanto nell'organizzazione e nella struttura, quanto nel *modus operandi*. Infatti la criminalità internazionale, così come il terrorismo di matrice islamica, fa costante uso della tecnologia ad esempio a fini di propaganda o d'istruzione degli adepti, oppure utilizza direttamente lo strumento dell'Internet al fine di perpetrare i reati stessi (si pensi a quanto in questi ultimi anni si sia ampliata la categoria dell'area relativa al *cyber-crime*).

In secondo luogo rileva il costante aggiornamento e l'evoluzione del fattore tecnologia.

Infatti il processo tecnologico e di globalizzazione ha mutato significativamente le modalità di raccolta, consultazione, utilizzazione, conservazione e trasferimento dei dati personali[212].

[212] Si pensi solamente in tema di conservazione, quale innovazione è stata il sistema di *Cloud and Cloud computing*, anche detta "nuvola informatica" che rappresenta un paradigma di erogazione di risorse informatiche, come l'archiviazione, l'elaborazione o la trasmissione di dati, caratterizzato dalla disponibilità *on-demand* attraverso Internet a partire da un insieme di risorse preesistenti e configurabili.

Sempre più frequente è la tendenza ad utilizzare, tanto a scopo commerciale, quanto nel settore della giustizia e della sicurezza, il patrimonio informativo derivante da trattamenti applicati negli ambiti più disparati[213]. Lo scopo che si vuole raggiungere è quello di «*munirsi di strumenti che permettano l'analisi comparativa di informazioni raccolte in contesti diversi, per individuare legami tra soggetti "noti" e persone non sospettate di reati, monitorarne gli spostamenti, elaborare criteri valutativi e di profilassi e, addirittura, formulare previsioni sui comportamenti individuali.*[214]».

Per confrontarsi in maniera adeguata alle nuove sfide imposte dal tempo e dall'evoluzione di fattori importanti per la cooperazione tra gli Stati membri «*occorrono norme aggiornate, chiare, coerenti e uniformi, che garantiscano la certezza del diritto e, di conseguenza, accrescano la reciproca fiducia.*[215]».

Condizione essenziale, affinché si possa creare un efficace scambio informativo tra Paesi, è la necessità di porre le basi per la creazione di uno spazio giuridico unitario che condivida principi di base comuni, livelli di protezione equivalenti e garanzie adeguate su tutto il territorio europeo.

Nel caso di computer collegati in rete locale (LAN) o geografica (WAN) la possibilità di elaborazione/archiviazione/recupero può essere estesa ad altri computer e dispositivi remoti dislocati sulla rete stessa. Sfruttando la tecnologia del *cloud computing* gli utenti collegati ad un *cloud provider* possono svolgere tutte queste mansioni, anche tramite un semplice internet browser.
Possono, ad esempio, utilizzare software remoti non direttamente installati sul proprio computer e salvare dati su memorie di massa on-line predisposte dal provider stesso (sfruttando sia reti via cavo che senza fili). In tema si veda GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2012 sul *Cloud computing*, (WP196), 1 luglio 2012.

[213] Si prenda ad esempio la DIRETTIVA UE 2016/681 del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) dei passeggeri dei voli in arrivo o in partenza dal territorio degli Stati membri, a fini di prevenzione, accertamento, indagine e azione penale per i reati di terrorismo e altri gravi reati. I PNR sono definiti dalla Direttiva come «*le informazioni relative al viaggio di ciascun 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*». In questo modo per gli scopi di cooperazione in materia giudiziaria e di polizia sono trattati e utilizzati dati che sono recepiti da compagnie e aziende private, dunque al di fuori dell'ambito istituzionale delle autorità competenti.

[214] P. TROISI, La protezione dei dati trattati a fini di prevenzione e accertamento dei reati, op. cit., p. 328.

[215] *Ibidem.*

Negli stessi termini si è pronunciato il Consiglio Europeo nel Programma di Stoccolma[216] determinando l'obiettivo di «*realizzare un regime completo di protezione, che includa anche la cooperazione penale e si fondi su principi di base quali la limitazione delle finalità, la proporzionalità, la legittimità del trattamento e la durata limitata della conservazione, in modo da garantire la sicurezza delle informazioni ed il rispetto dei diritti della persona, anche attraverso il controllo affidato ad organi nazionali di vigilanza indipendenti e l'accesso a effettivi mezzi di ricorso giurisdizionale*[217]».

Anche la Commissione europea e il Parlamento europeo si sono espressi in tal senso augurandosi l'estensione delle norme generali sulla protezione dei dati personali ai settori della cooperazione di polizia e giudiziaria[218], specialmente per quanto riguarda il trattamento a livello nazionale (c.d. domestico) escluso dal campo d'applicazione della Decisone quadro 977/2008/GAI, principale strumento normativo in tema.

La Direttiva UE 2016/680 è volta a disciplinare il 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, allo scopo di tutelare i diritti e le libertà fondamentali delle persone (in particolare, il diritto alla protezione dei dati) e di garantire, nel contempo, lo scambio di informazioni all'interno dell'Unione[219].

---

[216] PROGRAMMA DI STOCCOLMA, *Un' Europa aperta e sicura al servizio e a tutela dei cittadini* (2010/C 115/01), 4 maggio 2010. Il "Programma di Stoccolma" è il terzo programma di lavoro quinquennale dell'Unione europea in materia di Libertà, Sicurezza e Giustizia, dopo quelli di Tampere del 1999 e dell'Aia del 2004. E' stato approvato nel dicembre 2009 dal Consiglio europeo, cioè l'istituzione UE in cui si riuniscono gli Stati membri, rappresentati ai massimi livelli (capi di Stato o di governo).
Si tratta di un programma molto lungo e dettagliato, non vincolante per gli Stati: esso rappresenta piuttosto l'agenda che innanzitutto la Commissione, ma anche altre istituzioni europee (Parlamento europeo e Consiglio UE) devono seguire per orientare il loro lavoro in questo campo per gli anni 2010-2014.

[217] *Ibidem*, Programma di Stoccolma punto 2.5.

[218] Si tratta del documento della Commissione europea COM (2010) 609 del 4 novembre 2010, realizzato in esecuzione delle direttive contenute nel Piano d'azione per l'attuazione del Programma di Stoccolma e della Risoluzione del Parlamento europeo 2011/2025 (INI) del 6 luglio 2011 su *Un approccio globale alla protezione dei dati personali nell'Unione europea*.

[219] DIRETTIVA (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità

In questa Direttiva è superato uno dei limiti maggiori evidenziati dalla dottrina nella precedente normativa (Decisione quadro 2008/977/GAI). Infatti ora l'ambito d'applicazione non è più confinato al solo trattamento transfrontaliero, in quanto le varie attività di raccolta, registrazione, consultazione, trasmissione, diffusione, raffronto, interconnessione, cancellazione e distruzione, automatizzate e non, di dati contenuti in archivio o destinati a figurarvi, si applicano anche al trattamento *purely domestic* (quindi anche a livello nazionale o domestico). Si fonde dunque per la prima volta in un'unica disciplina il trattamento dei dati transfrontaliero e trattamento nazionale.

Se da un lato la Direttiva sembra predisporre delle buone basi per uniformare la materia, dall'altro lato però lascia "sopravvivere" le disposizioni specifiche degli atti dell'Unione precedenti[220], non contribuendo ad eliminare l'attuale frammentazione normativa.

Sono inclusi, nell'ambito d'applicazione della normativa, anche i trattamenti di dati personali ai fini della "*salvaguardia e prevenzione di minacce alla pubblica sicurezza*". Inciso, quest'ultimo, che spesso ha causato problemi esegetici, in quanto il concetto in esame si presta a svariate attività e a diverse interpretazioni.

Secondo quanto riportato dal Considerano n. 12 si accoglie una nozione ristretta di pubblica sicurezza in cui rientrano «*Le attività svolte dalla polizia o da altre autorità preposte all'applicazione della legge (…)in occasione di manifestazioni, grandi eventi sportivi e sommosse.*» nonché «*il mantenimento dell'ordine pubblico quale compito conferito alla polizia o ad altre autorità incaricate dell'applicazione della legge ove necessario per la salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica e agli interessi fondamentali della società tutelati dalla legge che possono dar luogo a reati.*». Rientrano inoltre il trattamento di dati effettuati dalle autorità competenti a seguito di una *notitia criminis* per l'indagine, accertamento e perseguimento dei reati, il

competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio, articolo 1.

[220] *Ibidem*, articolo 60.

trattamento senza la previa notizia di un fatto penalmente rilevante se rilevante al fine della prevenzione di reati. Ogni altro trattamento diverso, compiuto dalle stesse autorità per finalità ulteriori, è soggetto alle norme più rigide del Regolamento UE 2016/679.

La Direttiva generale UE 2016/680 raccoglie i principi base della disciplina sulla protezione dei dati personali, prendendo spunto dalle vecchie normative cardine del settore, ma rielaborandole e ricollocandole in un'ottica congiunta a quella del Regolamento UE 2016/679, portando avanti l'evoluzione del sistema da un impianto a tutela successiva-riparatoria, ad uno a tutela preventiva-precauzionale. In ogni caso la Direttiva elabora alcune differenze, rispetto a quanto stabilito dal Regolamento generale, "connaturali" al settore nel quale esplica i propri effetti.

Anzitutto i criteri di ***liceità e correttezza*** del trattamento nel settore penale risultano essere meno rigidi rispetto alla disciplina regolamentare, non includendo il consenso dell'interessato. L'articolo 8 prevede che il trattamento è definito lecito «*solo se e nella misura in cui è necessario per l'esecuzione di un compito di un'autorità competente (...) e si basa sul diritto dell'Unione o dello Stato membro.*».

Il ***principio di finalità*** è aspetto fondamentale di tutti gli strumenti che regolano lo scambio di informazioni. La limitazione delle finalità si riflette, oltre che sui confini di utilizzabilità delle informazioni, anche sulla tipologia dei dati personali che possono essere raccolti e scambiati e sull'individuazione delle autorità legittimate all'accesso[221]. La Direttiva a riguardo non apporta significative variazioni, prevedendo che i dati personali debbano essere raccolti «*per finalità determinate, esplicite e legittime e trattati in modo non incompatibile con tali finalità*» ed essere «*adeguati, pertinenti e non eccedenti rispetto alle finalità per le quali sono trattati*» (art. 4, lett. b, c).

Per quanto riguarda l'utilizzo successivo dei dati, per ulteriori finalità, si distingue tra il trattamento da parte della stessa o altra autorità: nel primo caso, il trattamento per finalità diverse da quella originaria, è consentito se autorizzato

[221] P. TROISI, op. cit., p. 336.

dal diritto dell'Unione o dello Stato membro quando sia «*necessario e proporzionato a tale altra finalità conformemente al diritto UE o dello Stato membro*»; nel secondo caso, invece, è generalmente vietato il trattamento per finalità diverse, a meno che non sia autorizzato dal diritto UE o dello Stato membro, ma in questa circostanza si applicherà la disciplina più rigorosa del Regolamento n. 679.

Per quanto riguarda invece l'aspetto della ***qualità dei dati*** già la Decisione quadro 2008/977/GAI, prevedeva l'obbligo per le autorità di attuare un controllo sui dati come condizione preliminare alla trasmissione, assicurandosi che quest'ultimi fossero esatti, completi e nel caso aggiornati. La Decisione quadro però non prevedeva la differenziazione dei dati per categorie di persone interessate, esattezza e affidabilità delle informazioni, contrariamente a quanto previsto da altri strumenti normativi come la Raccomandazione R (87) 15 o le Decisioni Europol e Eurojust.

Infatti l'esigenza di stabilire regole di trattamento diverse per le informazioni relative a persone non coinvolte in procedimenti penali, prosciolte o assolte, è espressione di una fondamentale garanzia, in quanto una raccolta indifferenziata e un trattamento generalizzato, in ambito penale, è fortemente lesivo della presunzione di non colpevolezza (*rectius* principio di innocenza). Lacuna, questa, colmata dalla nuova Direttiva all'articolo 7, par. 1, dove prevede che «*i dati personali fondati su fatti siano differenziati, nella misura del possibile, da quelli fondati su valutazioni personali*» sancendo inoltre all'articolo 6 l'obbligo per il titolare del trattamento di operare, nella misura del possibile, una chiara distinzione tra i dati personali: delle persone per le quali vi siano fondati motivi di ritenere che abbiano commesso reati o stiano per commettere reati, le persone condannate per un reato, le vittime di reato o le persone che alcuni fatti autorizzano a considerare potenziali vittime di reato e i terzi coinvolti.

In tema di ***dati sensibili*** la Direttiva inserisce due novità fondamentalmente: una di forma, l'altra di contenuto. In tema di dati sensibili la regola generale è per il divieto di trattamento di tutti quei dati che rivelano l'origine razziale o etnica, le

opinioni politiche, le convinzioni religiose o filosofiche, le condizioni di salute e la vita sessuale, se non nel caso in cui sia strettamente necessario e la legislazione nazionale preveda adeguate garanzie. Anche se nel settore della cooperazione giudiziaria e di polizia, a differenza di quanto previsto dalla Direttiva Madre (95/46/CE), non è richiesto il consenso dell'interessato per consentire il trattamento dei dati.

La prima novità di forma consiste nella formulazione dell'articolo 10 che non prevede un divieto, ma sancisce in linea generale la possibilità del trattamento dei dati sensibili quando strettamente necessario, in previsione di garanzie adeguate per i diritti e le libertà dell'interessato o se autorizzato dal diritto UE o dello Stato membro, o in caso contrario, se sia necessario a salvaguardare un interesse vitale dell'interessato o altra persona fisica.

La seconda novità consiste invece nell'aver incluso all'interno del novero dei dati c.d. sensibili, anche i dati genetici e biometrici diretti ad identificare in modo univoco una persona fisica.

Per quanto riguarda la ***conservazione e la cancellazione dei dati*** non sembrano esserci particolari differenze con i precedenti strumenti normativi di settore e con il dettato regolamentare. La cancellazione dei dati dunque consegue alla verifica positiva dell'inesattezza del dato, nonché come corollario dei principi di legittimità, di finalità e di durata limitata della conservazione. Allora si prevede che si opti per la cancellazione dei dati senza ingiustificato ritardo qualora siano violate le disposizioni di cui agli articoli 4 (Principi applicabili al trattamento di dati personali «*devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati*»), 8 (Liceità del trattamento) e 10 (Trattamento di categorie particolari di dati) oppure quando ciò sia imposto da un obbligo legale del titolare del trattamento[222].

[222] Articolo 16, *Diritto di rettifica o cancellazione di dati personali e limitazione di trattamento*, Direttiva generale UE 2016/680.

In alternativa alla cancellazione si procede alla limitazione[223] del trattamento quando l'interessato contesti l'esattezza dei dati personali e nel contempo non sia possibile verificarne l'esattezza, o quando sia necessaria la conservazione a fini probatori.

Sotto l'aspetto della ***sicurezza dei dati*** e degli ***obblighi del titolare e del responsabile del trattamento***, si nota l'impronta della politica giuridica scelta dal legislatore europeo che, nel Regolamento UE 2016/679, sancisce quel "cambio di rotta", un approccio completamente nuovo alla tutela dei dati personali. Si è sottolineato più volte come il sistema si sia spostato da un paradigma successivo-riparatorio, ad uno preventivo-precauzionale ponendo come perno fondamentale della tutela il trattamento e la corretta applicazione dei suoi principi nel massimo dettaglio possibile, calibrando con scrupolosa precisione gli obblighi e le responsabilità degli agenti principali del trattamento (titolare e responsabile) e infine elaborando un efficiente sistema di misure di sicurezza che viene concepito a monte del trattamento con lo scopo di diminuire, se non eliminare del tutto, il rischio di lesioni gravi per i diritti degli interessati. In tal senso è previsto che il trattamento garantisca un adeguato livello di protezione e sicurezza, mediante l'adozione da parte tanto del titolare che del responsabile, di «*misure tecniche e organizzative adeguate da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali*». Una novità in tema, riportata anche nel Regolamento generale, consiste nell'obbligo del titolare in caso di *data breach* di notificare senza ingiustificato ritardo all'autorità di controllo e, nel caso la violazione sia capace di rappresentare un rischio elevato per i diritti e le libertà delle persone fisiche, la comunicazione andrà rivolta anche all'interessato.

Per quanto riguarda gli obblighi di titolare e responsabile del trattamento interessante è il dovere stringente, previsto all'articolo 24, di tenere un registro di tutte le categorie di trattamento e di registrare il tutto in un sistema automatizzato, al fine di poter verificare la liceità del trattamento e la connessa

[223] La Limitazione consiste fondamentalmente nell'operazione che nella Decisione quadro 2008/977/GAI veniva definita "Blocco" inteso come quel « *contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento futuro.*».

responsabilità di chi pone in essere il trattamento, di favorire l'autocontrollo e di garantire l'integrità e la sicurezza dei dati.

Un importantissimo punto di svolta è sicuramente rappresentato dall'introduzione anche nel settore della cooperazione giudiziaria e di polizia dei principi, inseriti già nel Regolamento, della *privacy by design* e della *privacy by default*, assicurando in tal modo che, tanto al momento di elaborazione dei mezzi del trattamento, sia durante il trattamento stesso (quindi in una fase di autentica progettazione), siano approntate quelle misure tecniche e organizzative idonee a garantire la protezione dei dati, e che per impostazione predefinita possano essere trattati esclusivamente i soli dati necessari per le finalità del trattamento.

Seguendo tale spirito d'innovazione sono stati introdotti anche gli istituti della *valutazione di impatto* ogni volta il trattamento (per sua natura, oggetto, finalità) presenti rischi specifici ed elevati per i diritti e le libertà dell'interessato, nonché l'istituto della *consultazione preventiva* con l'autorità di controllo quando si debba creare un nuovo archivio e, in base alle risultanze della valutazione pre-impatto, oppure se il tipo di trattamento utilizza tecnologie, procedure o meccanismi nuovi, i diritti e le libertà delle persone, risultano essere in serio pericolo.

I ***diritti delle persone*** a cui i dati si riferiscono sono notevolmente migliorati rispetto alla Decisione quadro del 2008 n. 977, prevedendo in un'ottica di maggiore chiarezza e completezza, quali informazioni devono essere sempre messe a disposizione dell'interessato e quali ulteriori informazioni devono essere fornite al fine di consentire l'esercizio dei diritti individuali (art. 13). Riconoscendo, inoltre, il diritto dell'interessato ad avere conferma che sia in corso un trattamento nei propri confronti e di conseguenza, per tramite del diritto d'accesso, avere la possibilità di verificare la natura dei dati trattati e la liceità del trattamento. Sono altresì confermati e rafforzati i tradizionali diritti alla rettifica, cancellazione e limitazione dei dati personali. Va comunque ricordato che i diritti dell'interessato, nel settore della pubblica sicurezza e della giustizia penale, più che in qualsiasi altro contesto, soffrono alcune limitazioni e/o deroghe. Si può

prevedere dunque che la comunicazione delle informazioni aggiuntive sia ritardata, limitata o addirittura esclusa, anche se in ogni caso tale limitazione deve comunque costituire una misura necessaria e proporzionata in una società democratica. Ancora si può negare il diritto di accesso, rettifica, cancellazione o limitazione al fine di salvaguardare e non compromettere indagini, inchieste o procedimenti giudiziari, anche se in questi casi è sempre previsto che l'interessato interpelli l'autorità di controllo nazionale per verificare la liceità del trattamento, informandoli in seguito dell'avvenuta verifica.

Notevolmente aggiornata risulta essere anche la disciplina del ***trasferimento a paesi terzi o a organizzazioni internazionali*** che segue quanto già determinato dal Regolamento generale UE 2016/679. In quest'ambito è forte l'eco della vicenda giurisprudenziale *Schrems*[224] in cui la Corte di giustizia ha rielaborato in maniera ancor più netta il principio della *adequacy* per cui è essenziale che il Paese terzo assicuri effettivamente un livello di protezione dei diritti fondamentali sostanzialmente equivalente a quello garantito nell'ordinamento giuridico dell'Unione. Il trasferimento secondo quanto previsto dalla Direttiva può avvenire esclusivamente per i fini di cui all'articolo 1 (prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica), se l'autorità ricevente sia competente per dette finalità e se lo Stato membro che ha messo a disposizioni i dati ha fornito la propria autorizzazione preliminare al trasferimento. Sono inoltre rilevanti la decisione di adeguatezza della Commissione e l'autorizzazione dell'autorità competente che originariamente ha effettuato il trasferimento, nel caso in cui si voglia procedere ad un ulteriore trasferimento dei dati ad un altro Paese terzo o a un'altra organizzazione internazionale.

[224] CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), Sentenza nella causa C-362/14 Maximillian Schrems vs Data Protection Commissioner, Lussemburgo, 6 ottobre 2015.

Secondo quanto previsto dall'articolo 38 della Direttiva è possibile una deroga alla previa decisione di adeguatezza in alcune situazioni "limite" in cui sia necessario agire rapidamente, come quando il trasferimento sia necessario:

a) per tutelare un interesse vitale dell'interessato o di un'altra persona;
b) per salvaguardare i legittimi interessi dell'interessato;
c) per prevenire una minaccia grave e immediata alla sicurezza pubblica di uno Stato membro o di un Paese terzo;
d) nel singolo caso per le finalità di cui all'articolo 1 oppure per accertare, esercitare o difendere un diritto in sede giudiziaria.

Infine è previsto all'articolo 39 che in singoli casi e in presenza di condizioni tassative[225], il trasferimento possa essere effettuato direttamente a specifici destinatari stabiliti in paesi terzi che non siano autorità di *law enforcement*. La *ratio* sarebbe quella di *bypassare* le normali procedure che richiedono di

---

[225] Si riportano integralmente le condizioni tassative previste dall'articolo 39, par. 1, Direttiva UE 2016/680 "*In deroga all'articolo 35, paragrafo 1, lettera b), e fatti salvi eventuali accordi internazionali di cui al paragrafo 2 del presente articolo, il diritto dell'Unione o dello Stato membro può disporre che le autorità competenti di cui all'articolo 3, punto 7), lettera a), possano, in casi singoli e specifici, trasferire dati personali direttamente a destinatari stabiliti in paesi terzi soltanto se le altre disposizioni della presente direttiva sono rispettate e se sono soddisfatte tutte le seguenti condizioni:*

a) il trasferimento è strettamente necessario per l'assolvimento di un compito dell'autorità competente che opera il trasferimento ai sensi del diritto dell'Unione o dello Stato membro per le finalità di cui all'articolo 1, paragrafo 1;

b) l'autorità competente che opera il trasferimento determina che i diritti e le libertà fondamentali dell'interessato non prevalgono sull'interesse pubblico che rende necessario il trasferimento nel caso in questione;

c) l'autorità competente che opera il trasferimento ritiene che il trasferimento a un'autorità competente per le finalità di cui all'articolo 1, paragrafo 1, nel paese terzo sia inefficace o inadatto, in particolare in quanto il trasferimento non può essere effettuato tempestivamente;

d) l'autorità competente ai fini di cui all'articolo 1, paragrafo 1, nel paese terzo è informata senza ingiustificato ritardo, a meno che ciò sia inefficace o inadatto;

e) l'autorità competente che opera il trasferimento informa il destinatario della finalità specifica o delle finalità specifiche per le quali i dati personali devono essere trattati da quest'ultimo soltanto a condizione che tale trattamento sia necessario.".

contattare le autorità competenti del paese terzo, quando tali procedure possano essere inadatte o inefficaci, specialmente nel caso in cui gli ordinamenti siano così diversi da creare frizioni nel trasferimento in situazioni di particolare urgenza, per salvare la vita di una persona o per evitare un'imminente attentato terroristico sul territorio[226].

Nonostante le novità introdotte e le maggiori garanzie apportate, anche la Direttiva non è stata esente da critiche. Infatti si è ribadito come le ampie deroghe alla disciplina più garantista del Regolamento, fossero prive di giustificazione e non contribuissero a soddisfare l'auspicato requisito di un livello coerente ed elevato di protezione dei dati[227]. A riguardo la dottrina sottolinea come alcuni punti nevralgici non siano stati opportunamente sciolti:

a) manca un rafforzamento del principio di finalità, nella parte in cui non prevede la sempre maggiore capacità di interazione tra sistemi informativi creati con diverse funzioni e finalità;
b) non è in alcun modo disciplinato, neppure nel minimo, l'utilizzo dei dati raccolti da soggetti privati o da autorità non deputate all'applicazione della legge, da parte delle autorità di contrasto;
c) la nuova disciplina non elimina l'attuale e ormai perdurante frammentazione normativa del settore, lasciando in vita gli strumenti normativi precedenti dell'Unione, non incidendo nemmeno sui relativi accordi internazionali;
d) il trattamento domestico che rappresenta una delle maggiori novità rispetto al passato, non garantisce di per sé l'obiettivo di un livello di tutela equivalente in tutti gli Stati membri.

In ogni caso la stessa Dottrina è consapevole del fatto che «*scelte più coraggiose e ambiziose non si potevano pretendere in un settore, quello penale, "scosso" dalla emergenza terroristica e tradizionalmente oggetto di "riservato" dominio degli Stati, nonostante la prospettiva della realizzazione di uno "spazio di*

[226] Pressoché testuale il riferimento a P. TROISI, op. cit., p.348 e 349.
[227] Così si esprime il GARANTE EUROPEO DELLA PROTEZIONE DEI DATI nel *Parere* 2012/C192/05, del 7 marzo 2012 sull'intero pacchetto di riforma.

libertà, sicurezza e giustizia" abbia accelerato il processo di armonizzazione della normativa sia sostanziale che processuale[228]».

Nonostante, dunque, sembrerebbe un'armonizzazione minima quella apportata dalla Direttiva, a differenza del Regolamento, solo gli sviluppi successivi da parte dei legislatori nazionali dei vari Stati membri saranno capaci di contribuire alla realizzazione di un quadro generale e soddisfacente della protezione dei dati personali.

Sezione II

Le principali applicazioni giurisprudenziali tra istanze di sicurezza e tutela del diritto fondamentale alla protezione dei dati personali

1. Introduzione: la giurisprudenza a difesa dei diritti in stato di crisi

Mai, come in questo periodo storico, gli Stati occidentali si sono trovati a dover fronteggiare una minaccia costante come quella rappresentata dal terrorismo di matrice islamica. Una minaccia che denota peculiari caratteristiche non solo per le sempre più particolari modalità operative, ma specialmente per il bene al quale attentano. Infatti il *modus operandi* degli attacchi terroristici è cambiato notevolmente nei mezzi e negli strumenti adottati. Si pensi solamente all'utilizzo delle *Information and Communication Technology* (ICT), compresi i social networks, utilizzati a fine di propaganda, ma specialmente al fine di destabilizzare le istituzioni principali dei paesi tramite attacchi informatici ai sistemi centrali. Ancora, cambia totalmente la sorgente del pericolo. Fin dalla nascita della rete terroristica di Al Qaeda, il nemico era "facilmente" percepibile come un agente esterno, ora specialmente a seguito dell'avvento dell'Isis (e gli ultimi attentati sul suolo europeo ne sono la definitiva prova) il nemico assume contorni sempre più sfumati, le sue condotte sono sempre più imprevedibili,

[228] Così P. TROISI, op. cit., p. 353.

perché gli autori sono profondamente inseriti[229] nelle trame sociali degli Stati europei trattandosi, nella stragrande maggioranza dei casi di cittadini europei, figli di famiglie emigrate da generazioni, ma fortemente influenzabili dal fascino della concezione estremista del *jihad*.

È cambiato infine il bene al quale il terrorismo attenta. I bersagli principali degli attacchi non sono più strutture simbolo, monumenti o centri di potere dello Stato che si vuole colpire, ma il terrore è indirizzato in prima istanza verso la popolazione, cercando di creare un regime di paura costante capace di modificare in modo sostanziale le abitudini di vita dei cittadini. Ancora una volta ne sono un esempio lampante, gli ultimi attentati sul suolo europeo: a Parigi sono stati colpiti un teatro storico (il *Bataclan*), dei bar e dei ristoranti tra il X-XI *arrondissement* e lo *Stade de France*, a Nizza la via del lungomare (*La Promenade des Anglais*) è stata scenario di una folle corsa omicida di un tir, stessa dinamica dell'attentato avvenuto a Berlino ad un mercatino di natale, e infine la recentissima esplosione di un ordigno all'interno della *Manchester Arena* al termine del concerto della pop star internazionale Ariana Grande.

In questi frangenti di perenne allarme, la risposta fisiologica degli ordinamenti democratici è quella di adottare misure speciali a carattere emergenziale e di polizia, al fine di fronteggiare minacce alla sicurezza nazionale e alla incolumità dei propri cittadini[230].

---

[229] Si fa riferimento qui alla figura dei c.d. *Lone Wolves* (i lupi solitari) ossia di quegli estremisti che raggiunti dal messaggio jihadista globale, si organizzano per divenire operativi negli stessi Paesi Occidentali in cui vivono, agendo da soli o in piccoli gruppi destrutturati, al di fuori di vere e proprie associazioni terroristiche, e che, dopo aver autonomamente acquisito informazioni circa l'uso di armi o esplosivi, si attivano per la realizzazione di attentati di matrice jihadista. Per l'analisi e l'evoluzione storica del terrorismo islamico dal 2001 fino ai giorni nostri, e per lo studio dell'impatto che le nuove forme di terrorismo hanno avuto sul nostro sistema penale si veda F. FASANI, *Terrorismo Islamico e diritto penale*, CEDAM, Pavia, 2016.

[230] Sul tema della sicurezza, terrorismo e diritti fondamentali la produzione letteraria è florida. Solo per citarne alcuni: M. CANNAVICCI, *Terrorismo e intelligence*, Cap. XXIII, in Anatomia del crimine in Italia: manuale di criminologia a cura di B. ZOLI, R. S. DE LUCA, C. MACRÌ, Milano, Ed. 2016; INTERNATIONAL JOURNAL, *Sicurezza, terrorismo e società*, Italian Team for Security, Terroristic Issues & Managing Emergencies, 2016; G. DE MINICO, *Internet and fundamental rights in time of terrorism*, in Rivista AIC n. 4/2015; S. LA PISCOPIA, *Strumenti di lotta al terrorismo internazionale. Dall'indagine tradizionale "post delictum"alle frontiere della "proactive investigation"*, in La Giustizia Penale, 2014; S. LA PISCOPIA, *Misure investigative speciali e diritti umani tra nuove strategie internazionali e recenti normative metropolitane antiterrorismo*, in La Giustizia Penale, 2015; M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un*

L'esempio principe dell'attuazione di misure di emergenza è senz'altro il *Patriot Act* Statunitense del 2001, varato a seguito degli attentati coordinati al Pentagono e alle Torri Gemelle dell'11 settembre, che introduceva un insieme di norme e strumenti per ampliare il controllo sui cittadini americani tramite la raccolta e l'analisi di un'ingente quantità di dati al fine di migliorare i controlli di sicurezza nazionale. Proprio dall'attuazione delle norme del *Patriot Act* prese piede il famoso scandalo *Datagate*, a seguito delle rivelazioni di Edward Snowden (all'epoca dipendente della *National Security Agency* -NSA), che svelavano la massiccia attività di raccolta e trattamento di dati riguardanti non solo cittadini americani, ma di tutto il mondo (compresi i primi ministri di tutta Europa), da parte delle agenzie di sicurezza nazionale americane, possibile anche grazie alla collaborazione delle tante società che offrono servizi di *Information and Communication Technology* situate sul suolo americano.

Negli ultimi due anni si sono aggiornate e introdotte anche in Europa molte normative[231], specialmente nel settore penale, che hanno inserito all'interno

---

anno dagli attacchi di Parigi), in *federalismi.it* n. 23/2016; F. FASANI, *Terrorismo Islamico e diritto penale*, CEDAM, Pavia, 2016; M. O'NEILL, *Terrorism and human rights- EU data protection framework*, Cap. IX, in *The Evolving EU Counter-Terrorism Legal Framework*, Routledge research in EU law, Oxford, 2012.

[231] In Italia ciò è avvenuto per il tramite del Decreto legge del 18 febbraio 2015, n. 7 (legge di conversione 17 aprile 2015, n.43) c.d. *anti-terrorismo*. Il Decreto Legge si concentra, con soluzioni anche analoghe a quelle adottate di recente da altri Paesi europei, quali la Francia, sull'aggiornamento delle misure di prevenzione e contrasto del terrorismo. **Il provvedimento prevede sul piano penale:**

- l'introduzione di una nuova figura di reato destinata a punire chi organizza, finanzia e propaganda viaggi per commettere condotte terroristiche (reclusione da tre a sei anni);
- la punibilità del soggetto reclutato con finalità di terrorismo anche fuori dai casi di partecipazione ad associazioni criminali operanti con le medesime finalità (l'art. 270-*quater* c.p. sanzionava solo il reclutatore);
- la punibilità, sul modello francese, di colui che si "auto-addestra" alle tecniche terroristiche (fino ad oggi era punito solo colui che veniva addestrato da un terzo – art. 270-*quinquies* c.p.);
- l'introduzione di specifiche sanzioni, di ordine penale ed amministrativo, destinate a punire le violazioni degli obblighi in materia di controllo della circolazione delle sostanze (i cd. "precursori di esplosivi") che possono essere impiegate per costruire ordigni con materiali di uso comune. **Sul piano degli strumenti di prevenzione, le misure contemplate comprendono:**
- la possibilità di applicare la misura della sorveglianza speciale di pubblica sicurezza ai potenziali "*foreign fighters*";
- la facoltà del Questore di ritirare il passaporto ai soggetti indiziati di terrorismo, all'atto della proposta di applicazione della sorveglianza speciale di p.s. con obbligo di soggiorno. Il provvedimento è sottoposto a convalida dell'Autorità Giudiziaria;
- l'introduzione di una figura di reato destinata a punire i contravventori agli obblighi conseguenti al ritiro del passaporto e alle altre misure cautelari disposti durante il procedimento di prevenzione. **Inoltre, lo schema di decreto si incarica di aggiornare gli strumenti di contrasto all'utilizzazione**

dell'ordinamento misure specifiche e particolari regimi speciali in tema di contrasto ai nuovi fenomeni di terrorismo, innalzando le misure di sicurezza e rafforzando gli strumenti utilizzati ai fini di indagine e prevenzione dei reati.

Misure di sicurezza e strumenti di contrasto che sono diventati sempre più invasivi della sfera della *privacy* dei cittadini, grazie soprattutto alle innovazioni tecnologiche degli ultimi tempi e alle modalità del loro impiego. Tralasciando l'ampliamento delle tradizionali misure di intercettazione, basti pensare ai sistemi di videosorveglianza sempre più ad ampio raggio, alle banche dati nazionali e istituite a livello europeo, alle tecniche sempre più raffinate di analisi dei *Big Data* e all'utilizzo dei captatori informatici da remoto[232] tramite l'impiego di *software trojan*[233].

Nonostante il panorama sociale e giuridico sia in costante e vorticosa evoluzione a seguito della contestuale crescita della minaccia terroristica, ciò «*non vuol dire che le tradizionali frontiere non debbano essere presidiate*[234]». Infatti in periodi storici in cui multipli atti di terrorismo mettono a repentaglio la vita dei cittadini e i pilastri della società, «*il sentimento della popolazione si indirizza verso una maggiore richiesta di misure di polizia e di prevenzione*» portando a

---

della rete *internet* per fini di proselitismo e agevolazione di gruppi terroristici. In particolare, vengono previsti:

- aggravamenti delle pene stabilite per i delitti di apologia e di istigazione al terrorismo commessi attraverso strumenti telematici;
- la possibilità per l'Autorità Giudiziaria di ordinare agli *internet provider* di inibire l'accesso ai siti utilizzati per commettere reati con finalità di terrorismo, compresi nell'elenco costantemente aggiornato dal Servizio Polizia Postale e delle Telecomunicazioni della Polizia di Stato. Nel caso di inosservanza è la stessa Autorità Giudiziaria a disporre l'interdizione dell'accesso ai relativi domini *internet*.

ALTALEX, *Decreto Anti terrorismo: il testo*, in www.altalex.com, 21 aprile 2015. Per un'analisi approfondita sulle novità introdotte dal Decreto Legge 7/2015 a livello sostanziale e processuale penale si veda anche F. FASANI, *Terrorismo islamico e diritto penale*, op. cit., 2016.

[232] Tale tecnica di intercettazione da remoto è stata oggetto di una recentissima pronuncia della Corte di Cassazione Italiana che in tema ha adottato quantomeno conclusioni d'avanguardia nel settore dei "moderni metodi" di intercettazione. Cass., Pen., Sez. un., sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889.

[233] Nello specifico i software trojan, come captatori informatici, sono utilizzati sottoforma di virus tramite l'invio di email, messaggi o il download di applicazioni dalla rete e installati da remoto sui telefoni cellulari e tablet delle persone sospettate, con l'intento di registrare le conversazioni captate. M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it* n. 23/2016.

[234] *Ibidem*, p. 3.

«*considerare favorevolmente il potenziamento degli strumenti di controllo e protezione*[235]», anche se a discapito di posizioni di diritto consolidate.

In questo senso la giurisprudenza della Corte Europea dei Diritti dell'Uomo e della Corte di Giustizia Europea, così come quella delle Corti nazionali, hanno svolto un ruolo fondamentale in qualità di interpreti e garanti dei diritti fondamentali.

I giudici sovranazionali e nazionali sono sempre stati molto attenti nell'opera di bilanciamento, caso per caso, dei diversi interessi in gioco, cercando di elaborare la soluzione più efficiente al fine di soddisfare la pressante richiesta di sicurezza da una parte, e la difesa del nucleo essenziale dei diritti di volta in volta suscettibili di gravi lesioni, dall'altra.

Privacy e Protezione dei dati personali sono entrambi diritti che si sono evoluti e affermati a livello giurisprudenziale, e che continuano ad assumere sempre nuove sfumature, specialmente a fronte delle sfide poste dal terrorismo, grazie anche ad un costante e dinamico dialogo tra Legislatore e Corti.

2. La giurisprudenza della CEDU: i casi Uzun c. Germania (2010) e Szabó, Vissy c. Ungheria (2016)

Benché l'ordinamento CEDU non preveda espressamente un diritto fondamentale alla protezione dei dati personali, tale tutela a livello giurisprudenziale è stata attuata in parte tramite l'adesione alla Convenzione n. 108/1981 del Consiglio d'Europa "*sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale"* e in parte tramite un'interpretazione estensiva del diritto alla vita privata e familiare sancito dall'articolo 8 CEDU, comprensivo anche della protezione dei dati personali[236].

[235] *Ibidem*, p. 24.

[236] La Corte EDU ha da sempre posto una particolare attenzione alla tutela del "diritto al rispetto della vita privata e familiare" ex art. 8 CEDU, soprattutto nel rapporto con le esigenze di prevenzione e accertamento dei reati, nonché di sicurezza. Ad esempio si riportano di seguito: *Malone c. Regno Unito*, sent. 2 agosto 1984; *Kruslin c. Francia*, sent. 24 aprile 1990; *Rotaru c. Romania*, sent. 4 maggio 2000; *Taylor-Sabori c. Regno Unito*, sent. 22 ottobre 2002; *Peck c. Regno Unito*, sent. 28 gennaio 2003; *Perry*

Più volte la Corte di Strasburgo si è trovata nella situazione di dover analizzare e decidere quando, per esigenze di sicurezza nazionale, le intromissioni nella sfera privata degli individui fossero giustificate e proporzionate in base alle circostanze del fatto e degli strumenti utilizzati.

Un esempio importante il tal senso è il caso *Uzun c. Germania* del 2010[237], poiché per la prima volta la Corte EDU, analizzava la questione di una sorveglianza tramite strumentazione GPS[238].

Il ricorrente dal 1993 era sospettato di aver partecipato ai reati commessi dalla cosiddetta Cellula Anti-imperialista (*Anti-imperialistische Zelle*), un'organizzazione che perseguiva il combattimento armato, separata dal 1992 dalla Frazione delle Armate Rosse (*Rote Armee Fraktion*), un movimento terrorista di estrema sinistra. A seguito di tali sospetti il ricorrente veniva tenuto occasionalmente sotto sorveglianza visiva da parte dei membri del Dipartimento per la Tutela della Costituzione, gli ingressi nei suoi appartamenti venivano filmati con videocamere. Erano inoltre disposte le intercettazioni delle telefonate nella casa in cui il ricorrente viveva con sua madre e in una cabina telefonica situata nelle vicinanze. Anche la posta a lui indirizzata veniva aperta e controllata. Similmente, S., un presunto complice del ricorrente, veniva sottoposto a misure di sorveglianza dal 1993. Nell'ottobre 1995 la Procura Generale Federale avviava procedure investigative nei confronti del ricorrente e di S. per la partecipazione agli attentati dinamitardi dei quali la Cellula Anti-imperialista reclamava la responsabilità. L'Ufficio Federale per le indagini penali veniva incaricato delle indagini. Successivamente, il ricorrente e S. venivano

---

c. Regno Unito, sent. 17 luglio 2003; *Matheron c. Francia*, sent. 29 marzo 2005: *Vetter c. Francia*, sent. 31 maggio 2005; *Copland c. Regno Unito*, sent. 3 aprile 2007; *K. c. Finlandia*, sent. 2 dicembre 2008; *S. e Marper c. Regno Unito*, sent. 4 dicembre 2008; *Haralambie c. Romania*, sent. 27 ottobre 2009; *Bouchacourt c. Francia* e *M.B. c. Francia*, sent. 17 dicembre 2009; *M.K. c. Francia*, 18 aprile 2013.

[237] CORTE EUROPEA DEI DIRITTI DELL'UOMO, Quinta sezione, Sentenza *Uzun c. Germania*, n. 35626/05, 2 settembre 2010.

[238] Secondo il punto 13 della Sentenza della Corte EDU un sistema GPS è «*un sistema di navigazione-radio che lavora con l'aiuto dei satelliti. Esso permette la localizzazione continua, senza perdita di tempo, degli oggetti equipaggiati con un satellite GPS ovunque sulla terra, con una tolleranza massima di 50 metri alla volta. Esso non include una sorveglianza visiva o acustica. Al contrario dei trasmettitori, il suo utilizzo non necessita della conoscenza di dove si può trovare approssimativamente la persona da localizzare.*».

tenuti sotto sorveglianza visiva dai funzionari statali dell'Ufficio Federale per le indagini penali, principalmente durante i fine settimana tra il 30 settembre 1995 e il loro arresto avvenuto il 25 febbraio 1996. L'ingresso della casa in cui il ricorrente viveva con la madre era sorvegliato attraverso videocamere aggiuntive installate dall'Ufficio Federale per le indagini penali (da ottobre 1995 a febbraio 1996). Inoltre i telefoni di quella casa, di una cabina telefonica situata nelle vicinanze e dell'appartamento di S. ad Amburgo erano tenuti sotto controllo in base ad un provvedimento del giudice per le indagini della Corte Federale di Giustizia (dal 13 ottobre 1995 al 27 febbraio 1996). Lo stesso giudice ordinava alla polizia la sorveglianza del ricorrente e di S. così come delle auto da loro usate. Il controllo sulle auto utilizzate dai due sospettati avveniva in base all'installazione di due trasmettitori (*Peilsender*) nell'auto di S.

Tuttavia, il ricorrente e S. scoprivano e distruggevano i trasmettitori. Quando sospettarono che le loro comunicazioni venissero intercettate e che fossero sorvegliati, i due sospettati decisero di interrompere le comunicazioni telefoniche, sfuggendo anche alla video sorveglianza delle autorità investigative. Alla luce di ciò, l'Ufficio Federale per le indagini penali inseriva un dispositivo satellitare GPS (*Global Positioning System*) nell'auto di S. nel dicembre 1995, dietro ordine della Procura Generale federale. In tal modo si poteva determinare il luogo e la velocità dell'auto al minuto. Tuttavia i dati venivano recuperati a giorni alterni per prevenire la scoperta del satellite. Questa sorveglianza durava fino all'arresto del ricorrente e di S. il 25 febbraio 1996.

Dopo aver esaurito i rimedi interni il sig. Uzun ricorreva presso la Corte EDU, per far valere l'inutilizzabilità delle prove ottenute mediante la sorveglianza GPS all'interno del processo penale instaurato nei suoi confronti perché lesive del suo diritto fondamentale al rispetto della vita privata. Il ricorrente inoltre sosteneva che l'articolo 100c § 1 n°1 (b) del codice di procedura penale tedesco non potesse essere considerata una base giuridica sufficientemente precisa per la sua sorveglianza con l'aiuto del GPS. Non esisteva alcun controllo giurisdizionale effettivo su questa misura e l'uso contemporaneo di diversi mezzi di

sorveglianza, oltre a non rispettare il principio di proporzionalità, avrebbe dovuto basarsi su una diversa disposizione di legge. Inoltre, l'utilizzazione nel processo delle informazioni ottenute attraverso le suddette misure senza una base nell'ordinamento avrebbe violato il suo diritto a un equo processo. Tutte questioni rigettate in toto nel merito dalla Corte d'Appello di Düsseldorf, dalla Corte federale di Giustizia e infine dalla Corte Costituzionale Federale.

La Corte EDU nell'esaminare le questioni riportate dal ricorrente e dal Governo tedesco decise di prendere in considerazione i seguenti elementi:

a) Sulla questione dell'ingerenza nella vita privata, verificò prima se questa misura avesse rappresentato una raccolta di dati sul ricorrente, lesiva dell'articolo 8 CEDU;
b) Sulla questione se l'ingerenza fosse giustificata, verificò se l'ingerenza fosse stata prevista dalla legge nonché sullo scopo e sulla necessità di tale ingerenza.

Rispetto al punto a) il Governo asseriva che una raccolta dati ai danni del ricorrente non fosse avvenuta in quanto il ricevitore GPS era stato installato su di un oggetto, l'automobile, appartenente tra l'altro ad una terza persona (il complice S.). A tal proposito la Corte notò come l'applicazione del sistema GPS sulla vettura di S. aveva il preciso scopo di ottenere informazioni sui spostamenti del ricorrente e del suo complice e come l'utilizzo di quelle informazioni sia stata la base per porre in essere ulteriori indagini e raccogliere prove sui luoghi dove i due soggetti sono stati tracciati, avendo registrato i dati personali sistematicamente e avendoli usati per tracciare uno schema probatorio, utilizzato successivamente in tribunale. La Corte tuttavia sottolineava come «*la sorveglianza via GPS, per sua stessa natura, va distinta dagli altri metodi di sorveglianza visiva o acustica che sono, di regola, maggiormente suscettibili di interferire nel diritto di un individuo al rispetto della propria vita privata, poiché essi rivelano più informazioni sulla condotta, sulle opinioni o sui sentimenti di un*

individuo[239]». In ogni caso secondo i principi della giurisprudenza costante, nel caso di specie la Corte rilevò un'ingerenza nella vita privata del ricorrente ex art. 8 CEDU nel trattamento e nell'utilizzazione dei dati così ottenuti.

Analizzando il punto b) invece la Corte EDU rilevò come l'ingerenza trovasse un fondamento nel diritto positivo tedesco, nello specifico, nella disposizione dell'articolo 100c § 1 n°1 (b) del codice di procedura penale, una disposizione che era facilmente accessibile a livello conoscitivo da parte del ricorrente. Nel decidere se le disposizioni sulla sorveglianza via GPS del ricorrente rispettassero il requisito della "prevedibilità", la Corte tenne conto della tesi del ricorrente, secondo cui l'espressione "altri mezzi tecnici speciali destinati allo scopo della sorveglianza", contenuta nell'articolo 100c § 1 n°1 (b) del codice di procedura penale, non sarebbe stata sufficientemente chiara e non potesse dirsi capace di ricoprire la sorveglianza via GPS, arrivando ad affermare la chiarezza della lettera della disposizione in analisi (articolo 100c § 1 n°1 (b)) e che i mezzi tecnici in questione ricomprendevano i metodi di sorveglianza che non sono né visivi né acustici, ma rivelatori di posizione. La Corte riteneva dunque che «*la decisione dei giudici nazionali, in base a cui tale tipo di sorveglianza* (GPS) *è compresa nell'articolo100c § 1 n°1 (b), è un'evoluzione ed una chiarificazione ragionevolmente prevedibile della suddetta disposizione del codice di procedura penale svolta attraverso l'interpretazione giudiziaria*[240]».

In tema di garanzie, a fronte di possibili abusi, a seguito della predisposizione di una sorveglianza tramite tecnologie GPS, il ricorrente lamentava l'assenza di una previsione che limitasse nel tempo la misura (in effetti al tempo dei fatti un'espressa previsione mancava, inserita solamente più tardi tramite la riforma dell'articolo 163f § 4 del codice di procedura penale che prevedeva inoltre l'autorizzazione di un giudice nel caso la sorveglianza implicasse una durata superiore ad un mese di tempo) e che la concessione della misura da parte del pubblico ministero, senza previa autorizzazione di un giudice, non avrebbe

[239] Punto 49, Sentenza cit.
[240] Punto 65, Sentenza cit.

configurato una garanzia adeguata rispetto a possibili abusi. La Corte rilevò come la durata della misura di sorveglianza sia stata soggetta ad un attento scrutinio di proporzionalità nel caso concreto, e come i giudici nazionali ne abbiano controllato il rispetto (avendo operato la sorveglianza saltuariamente durante i finesettimana quando avvenivano gli spostamenti dei due soggetti a mezzo dell'autovettura e non in maniera continuativa). Inoltre in merito ai motivi richiesti per ordinare la sorveglianza di un individuo tramite GPS, l'articolo 100c § 1 n°1 (b), § 2 del codice di procedura penale prevede che tale sorveglianza possa essere ordinata solo contro una persona sospettata di un reato di notevole gravità o, in circostanze molto limitate, contro una terza persona sospettata di essere in contatto con l'imputato, e se gli altri mezzi di individuazione dei luoghi in cui si trova l'imputato avessero minore prospettiva di successo o fossero più difficoltosi. La Corte anche su questo punto ritenne che «*il diritto interno predisponga delle norme abbastanza rigorose per autorizzare la misura di sorveglianza in questione.*[241]».

La Corte continuava nella sua analisi sancendo che, nonostante la misura sia stata autorizzata in aggiunta ad altre misure direttamente dal pubblico ministero, la posizione del ricorrente in termini di garanzie da eventuali abusi, non risultava essere stata lesa poiché già sulla base delle disposizioni in vigore all'epoca dei fatti la sorveglianza di un individuo via GPS non era esente da un controllo giudiziario. Infatti nel «*successivo processo penale contro la persona interessata, i giudici penali hanno potuto riesaminare la legittimità di tale misura di sorveglianza e, nel caso in cui la misura fosse stata ritenuta illegittima, avevano il potere* (di) *escludere le prove in tal modo ottenute dal processo*», la Corte per giunta ritenne che il «*riesame giudiziario e la possibilità di escludere le prove ottenute da una sorveglianza via GPS illegittima rappresenta un'importante garanzia. Alla luce del fatto che la sorveglianza via GPS deve essere considerata un'ingerenza minore nella vita privata di una persona rispetto, per esempio, all'intercettazione telefonica, la Corte ritiene che il successivo riesame*

[241] Punto 67, Sentenza cit.

giudiziario della sorveglianza di una persona mediante GPS offra una tutela sufficiente contro l'arbitrio»[242].

Infine i Giudici di Strasburgo nel decidere in merito allo scopo e alla necessità dell'ingerenza nel caso di specie, incentrarono l'analisi sul paradigma di ciò che bisogna reputare necessario "in una società democratica". La Corte ricordava che la nozione di necessità significa che l'ingerenza corrisponde ad un bisogno sociale impellente e, in particolare, che è proporzionata rispetto allo scopo legittimo perseguito.

Rispetto a questo contesto la sorveglianza via GPS non era stata autorizzata fin dall'inizio delle indagini e, ad ogni modo, era stata effettuata per un periodo di tempo relativamente breve (circa tre mesi) e a intervalli non regolari (in genere durante i finesettimana o durante i viaggi in auto con il complice S.) e solo esclusivamente quando gli altri metodi di sorveglianza si erano rivelati inadeguati o erano stati scoperti e distrutti dai due sospettati. Allo stesso modo non bisogna sottovalutare il fatto che le indagini per le quali la sorveglianza era stata richiesta riguardavano reati molti gravi, vale a dire vari tentati omicidi di politici e funzionari pubblici mediante attacchi dinamitardi. A seguito di tali conclusioni la Corte EDU ritenne infine che la sorveglianza del ricorrente via GPS, come realizzata nel caso di specie è stata proporzionata rispetto ai legittimi scopi perseguiti e, dunque, "necessaria in una società democratica" ai sensi dell'articolo 8, par. 2, e che non si è concretizzata una lesione dell'articolo 8 CEDU.

Un altro esempio importante, oggetto di una recente pronuncia della Corte Europea dei Diritti dell'Uomo, è rappresentato dal caso *Szabó e Vissy c. Ungheria*[243]. I due ricorrenti, Máté Szabó e Beatrix Vissy, cittadini ungheresi, al tempo dei fatti lavoravano presso un'organizzazione non governativa (*Eötvös Károly Közpolitikai Intézet*) contraria al governo ungherese e contro cui muoveva

[242] Punti 68 e 69, Sentenza cit.

[243] CORTE EUROPEA DEI DIRITTI DELL'UOMO, Sezione II, *Máté Szabó e Beatrix Vissy c. Ungheria*, sentenza n. 37138/14, 12 gennaio 2016. Per accedere al testo, disponibile solamente in lingua inglese, e consultare i dettagli della pronuncia si veda www.hudoc.echr.coe.int.

una forte attività di critica. Il 1 gennaio 2011, mediante l'adozione della legge n. CCVII, il governo ungherese istituiva una Task Force antiterrorismo all'interno delle forze di polizia le cui competenze, come originariamente previste dalla sezione 7/E della legge n. XXXIV del 1994 sulla Polizia, venivano modificate dalla legge del 2011. In base a queste nuove modifiche i poteri della task force nell'ambito della raccolta di informazioni e intelligence comprendevano anche ricerche occulte e segrete presso le abitazioni, la sorveglianza attraverso sistemi di registrazione (video e audio), il controllo e l'apertura della corrispondenza nonché la captazione e la registrazione dei contenuti delle comunicazioni elettroniche e informatiche, tutto ciò senza il consenso della persona interessata.

I ricorrenti, anche se non direttamente colpiti da suddette misure, ma temendo la possibilità di essere sottoposti a sorveglianza a causa della loro azione di contrasto e critica aperta al governo magiaro, nel giugno 2012 presentarono un ricorso alla Corte costituzionale ungherese sostenendo che i nuovi poteri elargiti alla polizia nell'ambito della lotta al terrorismo, ai sensi delle modifiche alla sezione 7/E, violassero il diritto al rispetto della vita privata e familiare ex articolo 8 CEDU.

La Corte Costituzionale respinse la maggior parte dei ricorsi, solo un aspetto delle lamentele riportate trovò concorde la Corte. La decisione del ministro di giustizia ungherese che ordinava la raccolta di informazioni e di intelligence, specialmente se da attuare mediante modalità segrete, non poteva avvenire "in bianco", ma necessitava di ragioni e prove a fondamento della necessità dell'attuazione delle misure. Il 13 maggio del 2014 i due ricorrenti adirono la Corte europea dei diritti dell'uomo, continuando a sostenere che il loro diritto alla privacy, come quello di tutti i cittadini ungheresi, non fosse adeguatamente protetto dalla normativa del 2011, mancando tra l'altro una qualsiasi forma di controllo o rimedio giudiziale in merito all'autorizzazione di tali misure di sicurezza.

In primo luogo, la Corte confermava la rilevanza della questione, in termini di incidenza al diritto fondamentale sancito dall'articolo 8 CEDU da parte della

normativa ungherese, e rilevava come la normativa d'emergenza fosse capace di toccare indistintamente tutti gli utenti dei sistemi di comunicazione senza prevedere la possibilità da parte di quest'ultimi di poter presentare una denuncia ad un organismo indipendente. Non era in discussione tra le parti la conformità dell'obiettivo proposto dal *Police Act* ungherese di salvaguardare la sicurezza nazionale e / o di prevenire disturbi o crimini gravi, e tanto meno in dubbio era la base giuridica di riferimento. Infatti la Corte accertò che le due situazioni per le quali erano consentite le severe misure di sorveglianza segreta a fini di sicurezza nazionale e ai sensi del diritto interno (e cioè il pericolo rappresentato dal terrorismo e la necessità di intraprendere operazioni di salvataggio dei cittadini ungheresi in difficoltà all'estero) erano sufficientemente chiare.

Tuttavia, la Corte non era convinta che la legislazione ungherese fornisse adeguate garanzie in termini di precisione, efficacia e completezza in merito all'ordine, all'esecuzione e alla rettifica di tali misure. Ciò specialmente perché mancava all'interno della normativa alcuna descrizione specifica ad esempio delle categorie di persone che potevano essere sottoposte a tali misure in forza di qualche concreto sospetto, ingenerando così il timore che qualsiasi persona arbitrariamente potesse essere soggetta a sorveglianza segreta. Era infatti semplicemente sufficiente che le autorità competenti indicassero al ministro di giustizia ungherese, anche solo una "gamma di persone" da intercettare, senza dover neppure dimostrare una reale o presunta relazione con una qualsiasi minaccia terroristica.

La Corte, secondo la sua costante giurisprudenza[244], ribadiva che qualsiasi misura di sorveglianza segreta, che non rispondesse al criterio della stretta necessità per

[244] Molti dei quali citati all'interno della sentenza, come ad esempio: *Amann v. Switzerland* [GC], no. 27798/95, §§ 56-58, ECHR 2000 11*; Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, 28 June 2007; *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007 I; *Dumitru Popescu v. Romania* (no. 2), no. 71525/01, 26 April 2007*; Esbester v. the United Kingdom*, no. 18601/91, Commission decision of 2 April 1993; *Gustafsson v. Sweden*, 25 April 1996, § 51, Reports of Judgments and Decisions 1996 II; *Halford v. the United Kingdom*, 25 June 1997, §§ 56 to 57, Reports 1997 III; *Huvig v. France*, 24 April 1990, Series A no. 176 B*; Iliya Stefanov v. Bulgaria*, no. 65755/01, § 49, 22 May 2008; *Iordachi and Others v. Moldova*, no. 25198/02, 10 February 2009; *Kennedy v. the United Kingdom*, no. 26839/05, 18 May 2010; *Klass and Others v. Germany*, 6 September 1978, Series A no. 28; *Kokkinakis v. Greece*, 25 May 1993, § 40, Series A no. 260 A; *Kopp v.*

la salvaguardia delle istituzioni democratiche o per l'ottenimento di intelligence vitale in un'operazione, non poteva essere ammessa. Un altro elemento che la Corte rilevò come sintomo di potenziale abuso del diritto alla riservatezza dei cittadini ungheresi era la durata della sorveglianza, poiché era dubbio il regime di proroghe della durata delle misure di sorveglianza (era difficile capire se l'iniziale durata di 90 giorni potesse essere prorogata per ulteriori 90 giorni una sola volta oppure ripetutamente). Inoltre la Corte EDU sottolineò come la supervisione e l'autorizzazione in capo ad un responsabile dell'esecutivo (il ministro di giustizia), senza il preliminare scrutinio di un'autorità giurisdizionale o di un'autorità indipendente in merito alla necessità e alla proporzionalità delle misure di sorveglianza segreta da porre in essere, non garantisse efficacemente la protezione delle persone contro eventuali abusi. Solo un controllo giudiziario esterno è capace di offrire le migliori garanzie di indipendenza, imparzialità e di una corretta procedura.

In conclusione, dato che il campo d'applicazione delle misure previste si configurava di portata talmente estesa da riuscire ad includere qualsiasi cittadino ungherese; dato che l'ordine di esecuzione delle misure avveniva esclusivamente ad opera dell'esecutivo senza un previo controllo giurisdizionale o paragiurisdizionale; dato che l'ordine di esecuzione non era sorretto da evidenze probatorie in merito alla sussistenza di una reale minaccia, travalicando i principi di stretta necessità e proporzionalità; dato che le modalità di sorveglianza, per il loro elevato livello tecnologico erano capaci di intercettare facilmente masse di

---

Switzerland, 25 March 1998, Reports 1998 II; *Krone Verlag GmbH & Co. KG v. Austria* (no. 4), no. 72331/01, § 26, 9 November 2006; *Kruslin v. France*, 24 April 1990, § 27, Series A no. 176-A; *Kvasnica v. Slovakia*, no. 72094/01, 9 June 2009; *Lambert v. France*, 24 August 1998, § 23, Reports 1998-V; *Liberty and Others v. the United Kingdom*, no. 58243/00, 1 July 2008*; Malone v. the United Kingdom*, 2 August 1984, § 64, Series A no. 82; *Matthews v. the United Kingdom*, no. 28576/95, Commission decision of 16 October 1996*; N.C. v. Italy* [GC], no. 24952/94, § 56, ECHR 2002 X*; Nagla v. Latvia*, no. 73469/10, § 82, 16 July 2013*; Ostrovar v. Moldova*, no. 35207/03, § 113, 13 September 2005; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX (extracts); *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003*; Redgrave v. the United Kingdom*, no. 20271/92, Commission decision of 1 September 1993*; Roman Zakharov v. Russia*, [GC], no. 47143/06, 4 December 2015; *Társaság a Szabadságjogokért v. Hungary*, no. 37374/05, § 36, 14 April 2009; *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, no. 39315/06, § 101, 22 November 2012; *Valenzuela Contreras v. Spain*, 30 July 1998, § 46, Reports 1998 V.

dati riguardanti anche ulteriori soggetti rispetto all'originale "gamma di persone" sorvegliate e data l'assenza di rimedi efficaci per le violazioni o le lesioni subite,tanto sul piano amministrativo, quanto su quello giurisdizionale, la Corte EDU concluse in senso affermativo in merito all'esistenza di una violazione dell'articolo 8 della CEDU, da parte del Police Act ungherese del 2011.

3. La giurisprudenza della Corte di Giustizia Europea: il recentissimo caso Tele2 e Watson c. Regno Unito (2016)

L'ordinamento UE, diversamente dall'ordinamento CEDU, riconosce espressamente il diritto alla protezione dei dati personali come un diritto fondamentale sancito nell'articolo 16 del TFUE e nell'articolo 8 della Carta dei diritti fondamentali dell'Unione Europea, come declinazione dei diritti della personalità. Sul versante giurisprudenziale l'operato della CGUE è stato sicuramente uno dei più incisivi nella creazione del diritto alla protezione dei dati personali e nel tempo ha inanellato importanti sentenze che ne hanno contraddistinto il ruolo centrale sia come difensore, sia come principale soggetto dello sviluppo ed evoluzione della disciplina di settore. Basti pensare che molte delle novità introdotte nel nuovo "pacchetto della protezione dati" (composto dal Regolamento UE 2016/679 e dalla Direttiva UE 2016/680), corrispondono esattamente a deduzioni o ad auspici dei giudici di Lussemburgo, sviluppati in sentenze cardine. Basti citare a titolo esemplificativo la sentenza *Google Spain*[245] in cui la Corte, analizzando il rapporto tra dati personali e attività dei motori di ricerca, elabora una nuova declinazione del c.d. diritto all'oblio come diritto alla deindicizzazione delle informazioni. La Corte di Giustizia qualificando l'attività dei motori di ricerca come un effettivo trattamento di dati personali, riconduce

[245] CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), 13 maggio 2014, Sentenza nella causa C-131/12 *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González*, 2014. In tema si veda F. PIZZETTI, in *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, 2014; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Diritto dell'Informazione e dell'Informatica*, Giuffrè, Milano, 2014; G. RESTA – V. ZENO-ZENOVICH, *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015; S. SICA– V. D'ANTONIO, *La procedura di de-indicizzazione*, 2015.

l'espletamento di tale attività sotto l'ombrello della disciplina europea in materia di protezione dati. Da qui la possibilità di azionare anche i meccanismi di esercizio dei diritti, potendo l'interessato richiedere al motore di ricerca la soppressione di determinati collegamenti su pagine web di notizie, anche se legittimamente pubblicate, che nel tempo abbiano perso la propria rilevanza o siano mutate di contesto.

Ancora si pensi alla famosa sentenza *Schrems*[246], vicenda che ha avuto forte eco mediatico perché, prima di tutto, era coinvolta una delle piattaforme multimediali social più famosa del mondo (Facebook), poi perché la decisione della Corte comportò la cessazione dell'efficacia degli accordi USA-UE per il trasferimento di dati tra i due territori, chiamato *Safe Harbor*. Per la prima volta tramite una sentenza della Corte di Giustizia europea viene annullata una decisione[247] della Commissione europea, che in tema di trasferimento dei dati verso paesi terzi, doveva accertare il livello di *adequacy* rispetto alla protezione prevista dall'ordinamento UE. Principio di adeguatezza della tutela che secondo il ricorrente Maximillian Schrems non era rispettato dall'accordo *Safe Harbor* che, anche grazie alle indiscrezioni di un controllo globale da parte degli Stati Uniti d'America, trapelate a seguito dello scandalo Datagate, convinsero il cittadino austriaco ad intraprendere la via giudiziale, fino al rinvio pregiudiziale alla Corte di Giustizia europea. La Corte UE entra nel merito della decisione della Commissione valutandone i criteri adoperati e rileggendoli alla luce dei principi della protezione dei dati personali, arrivando a sancire l'inadeguatezza della protezione offerta dall'accordo in questione. La Corte di Giustizia oltre a

[246] CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), Sentenza nella causa C-362/14 Maximillian Schrems vsData Protection Commissioner, Lussemburgo, 6 ottobre 2015. In tema si rimanda a R. BIFULCO, *La sentenza Schrems e la costruzione del diritto europea alla privacy*, in *Giurisprudenza Costituzionale*, Anno LXI Fasc. 1, Milano, 2016; B. CAROTTI, *Il caso Schrems, del conflitto tra riservatezza e sorveglianza di massa – il commento*, in *Giornale Dir. Amm.*, 2016; D. MULA, *Trasferimento verso paesi terzi*, , Cap. XIV, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016, pag. 283; M. BONINI, *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: dei diritti" violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 2016; M. TRESCA, *Sicurezza vs protezione dei dati: la CGUE cambia registro*, in *Amministrazione In Cammino*, 2016.

[247] La decisione della Commissione europea in questione è la Decisione n. 520 del 26 luglio 2000.

confermare che le autorità Garanti non possono andare contro una decisione della Commissione (in primis per il tenore letterale dell'articolo 25, par. 6, Direttiva 95/46/CE nella parte in cui prevede che «*gli Stati membri adottano le misure necessarie per conformarsi alla decisione della Commissione*», in secundis per il principio del primato del diritto comunitario rispetto al diritto interno), rileva come sia necessario un sistema capace di limitare la discrezionalità della Commissione, prevedendo un elenco tassativo degli elementi per i quali è possibile rilasciare un *placet* di adeguatezza.

Un'altra sentenza di grandissimo rilievo è quella inerente al caso comunemente denominato *Digital Rights Ireland*[248] che invalida la direttiva 2006/24/CE, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura dei servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione. La Corte in questo caso stigmatizza in maniera netta e decisa la tendenza ad una *blanket data retention*, ossia ad un sistema di conservazione di massa dei dati, diffuso e generalizzato. La vicenda nasce a seguito di due rinvii pregiudiziali (uno da parte dei giudici di Irlanda, l'altro da parte dei giudici austriaci) che richiedevano una verifica in merito alla compatibilità della normativa della *data retention* rispetto ai diritti fondamentali alla riservatezza e alla protezione dei dati personali. La Corte in prima istanza verificò l'incidenza della normativa coi diritti di cui agli articoli 7 e 8 della Carta di Nizza e rilevò subito come l'obbligo generalizzato dei fornitori di conservazione dei dati comportava un'ingerenza di «*vasta portata (…) e particolarmente grave*[249]». La CGUE continuava, verificando se tale ingerenza potesse essere altrimenti giustificata alla luce dell'articolo 52 della Carta di Nizza, il quale può prevedere delle limitazioni dei diritti in tre specifiche situazioni: se previste dalla legge, se

[248] CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), 8 aprile 2014, Digital Rights Ireland Ltd (C-293/12) contro Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung (C-594/12) e altri,2014. In tema si veda per l'analisi dei punti chiave della Sentenza *Data Retention* M. TRESCA, *Sicurezza vs protezione dei dati: la CGUE cambia registro*, in *Amministrazione In Cammino*, 2016; si veda anche S. SICA, V. D'ANTONIO, G.M. RICCIO, *La Nuova Disciplina Europea della Privacy*, Milano, 2016 e F. PIZZETTI, *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Vol I de *I Diritti nella "rete" della Rete*, Torino, 2016.

[249] Punto 37 Sentenza cit.

rispettino il principio di proporzionalità e se siano necessarie per perseguire gli scopi di interesse generale. Secondo il parere della Corte di Giustizia europea due dei tre requisiti sarebbero soddisfatti, mentre il criterio di proporzionalità non passerebbe il vaglio dei giudici. Quest'ultimi censurarono la generalità del sistema di conservazione dei dati, nonché in generale delle disposizioni della direttiva, capaci di comportare un controllo pressoché di massa sulla popolazione europea, non fondato su alcun elemento di differenziazione in base alla sussistenza di sospetti nei confronti di una persona o dall'esistenza effettiva di un rischio per la sicurezza pubblica. La normativa mancherebbe di criteri oggettivi, di coerenza e specificità sotto multipli profili, come quello inerente l'accesso da parte delle autorità nazionali competenti in merito al controllo preventivo da parte di un giudice o un'autorità indipendente sullo stesso accesso e in merito alla stessa durata della conservazione. Anche se è facilmente intuibile che la normativa del 2006 potesse essere stata fortemente influenzata dagli attacchi terroristici di Madrid e Londra, la Corte affermò con fermezza che «*nessuna esigenza di sicurezza nazionale, e nel caso di specie neanche la minaccia terroristica, può giustificare un'ingerenza così generalizzata e indeterminata nei riguardi del diritto fondamentale alla protezione dei dati personali*».

È proprio dalla sentenza *Digital Rights Ireland* che prende piede la questione relativa alla causa *Tele 2 e Watson*[250].

Anche in questo caso si parla di due cause riunite: la prima (causa C-203/15) vede contrapporsi la *Tele2 Sverige AB* alla *Post- och telestyrelsen* (autorità svedese di sorveglianza delle poste e delle telecomunicazioni "PTS"), in merito ad un'ingiunzione con cui quest'ultima ha ordinato alla Tele2 di procedere alla conservazione dei dati relativi al traffico e dei dati relativi all'ubicazione dei suoi abbonati ed utenti iscritti; mentre la seconda (causa C-698/15) oppone i

[250] CORTE DI GIUSTIZIA EUROPEA, (Grande Sezione), *Tele2 e Watson*, cause riunite C-203/15 e C-698/15, sentenza 21 dicembre 2016. Si veda in proposito O. POLLICINO – M. BASSINI, *LA CORTE DI GIUSTIZIA E UNA TRAMA ORMAI NOTA: LA SENTENZA TELE2 SVERIGE SULLA CONSERVAZIONE DEI DATI DI TRAFFICO PER FINALITÀ DI SICUREZZA E ORDINE PUBBLICO*, nota a Corte Giustizia UE, sent. 21 dicembre 2016, Tele2 e Watson, cause riunite C-203/15 e C-698/15, 2017.

signori Tom Watson, Peter Brice e Geoffrey Lewis al *Secretary of State for the Home Department* (Ministro dell'Interno, Regno Unito di Gran Bretagna e Irlanda del Nord), in merito alla conformità al diritto dell'Unione, dell'articolo 1 del *Data Retention and Investigatory Powers Act* 2014 (DRIPA), legge inerente la conservazione dei dati e dei poteri di indagine.

Nonostante la questione vertesse sull'interpretazione dell'articolo 15 della direttiva 2002/58/CE[251] relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche, è forte il richiamo alle determinazioni della CGUE nella storica sentenza *data retention*. Infatti il paradigma elaborato dalla Corte con la contestuale invalidazione della direttiva 2006/24/CE ha comportato un clima di incertezza negli ordinamenti che l'avevano recepita.

Proprio riguardo la prima questione pregiudiziale veniva richiesto alla Corte di giustizia di chiarire se la disposizione di cui all'art. 15 della direttiva del 2002, letta alla luce della Carta dei diritti fondamentali dell'Unione europea, impedisse agli Stati membri di prevedere misure di conservazione generalizzata e indifferenziata dei dati di traffico e dei dati relativi all'ubicazione di abbonati e utenti di servizi di comunicazione elettronica. Nel primo procedimento era controversa la legittimità di un'ingiunzione adottata dall'autorità svedese delle

[251] L'articolo 15 della direttiva 2002/58/CE, intitolato "Applicazione di alcune disposizioni della direttiva 95/46/CE prevede che: «*1. Gli Stati membri possono adottare disposizioni legislative volte a limitare i diritti e gli obblighi di cui agli articoli 5 e 6, all'articolo 8, paragrafi da 1 a 4, e all'articolo 9 della presente direttiva, qualora tale restrizione costituisca, ai sensi dell'articolo 13, paragrafo 1, della direttiva 95/46/CE, una misura necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica. A tal fine gli Stati membri possono tra l'altro adottare misure legislative le quali prevedano che i dati siano conservati per un periodo di tempo limitato per i motivi enunciati nel presente paragrafo. Tutte le misure di cui al presente paragrafo sono conformi ai principi generali del diritto comunitario, compresi quelli di cui all'articolo 6, paragrafi 1 e 2, del trattato sull'Unione europea.*

2. Le disposizioni del capo III della direttiva 95/46/CE relative ai ricorsi giurisdizionali, alle responsabilità e alle sanzioni si applicano relativamente alle disposizioni nazionali adottate in base alla presente direttiva e con riguardo ai diritti individuali risultanti dalla stessa.

3. Il gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito dall'articolo 29 della direttiva 95/46/CE, svolge i compiti di cui all'articolo 30 della direttiva stessa anche per quanto concerne materie disciplinate dalla presente direttiva, segnatamente la tutela dei diritti e delle libertà fondamentali e degli interessi legittimi nel settore delle comunicazioni elettroniche.».

comunicazioni (PTS) sulla base della disciplina nazionale, con cui era stato ordinato a Tele2 di provvedere alla conservazione dei dati relativi alle comunicazioni elettroniche, conservazione cessata proprio al fine di ottemperare ai dettami enucleati nella sentenza *Digital Rights Ireland*. Dunque si chiedeva se una norma come l'art. 15 della direttiva 2002/58/CE esaurisse in modo puntuale il potere (legittimo) delle autorità nazionali di interferire con il diritto alla riservatezza[252].

Nella seconda questione pregiudiziale, invece, si richiedeva alla Corte se quanto contenuto all'interno dell'art. 15 impedisse agli Stati membri di prevedere un accesso ai dati personali da parte delle autorità nazionali competenti senza limitare tale accesso a finalità specifiche, come la lotta alla criminalità o al terrorismo, e senza sottoporlo a un previo controllo da parte dell'autorità giudiziaria o amministrativa. Nel secondo procedimento in via principale, infatti, era contestato il potere del Ministero dell'Interno britannico di imporre ai fornitori di servizi di comunicazione elettronica la conservazione dei dati per un periodo massimo di dodici mesi senza alcun preventivo scrutinio delle autorità competenti.

In merito alla questione sollevata dal conflitto tra Tele2 e la PTS la Corte rilevò come, da un lato, l'art. 1, par. 3, della direttiva 2002/58/CE escludesse dal proprio ambito di applicazione le materie della sicurezza pubblica, della difesa e dell'ordine pubblico; dall'altro, come l'art. 15 autorizzasse gli Stati membri all'adozione di misure che limitano la privacy, riferendosi però alle attività proprie degli Stati o delle autorità statali.

Tuttavia la Corte rimarcava come la norma suddetta costituisse un'eccezione rispetto al divieto di memorizzare dati di traffico senza il consenso degli utenti da parte di qualsiasi soggetto e che in ragione di ciò l'art. 15 deve formare oggetto di un'interpretazione restrittiva (ciò anche in base ai principi di finalità e minimizzazione dei dati). Ne consegue che gli Stati membri non possono

[252] O. POLLICINO – M. BASSINI, *LA CORTE DI GIUSTIZIA E UNA TRAMA ORMAI NOTA …,* cit., p. 5.

adottare misure che interferiscano con la riservatezza degli individui per perseguire finalità diverse da quelle espressamente menzionate dall'art. 15, par. 2 che le individua nelle misure necessarie, in una società democratica, a «*la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica, e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica*». A seguire la Corte di Giustizia europea non mancò di condurre uno scrutinio accurato in merito alla necessità di tale ingerenza e se fosse giustificata ex art. 52[253] della Carta dei diritti fondamentali dell'Unione europea. Essendo condizione ineludibile una lettura "costituzionalmente" orientata al rispetto dei diritti fondamentali la Corte rilevava come la disciplina controversa, legittimando una conservazione generalizzata e indifferenziata, in maniera continua e sistematica, sia dei dati relativi al traffico, sia dei dati relativi all'ubicazione di abbonati e iscritti in rapporto a tutti i mezzi di comunicazione elettronica, «*rievochi le misure previste dalla direttiva 2006/24/CE*[254]». Si qualifica dunque, in questo caso, un'ingerenza della normativa svedese nel diritto alla riservatezza e alla protezione dei dati personali, volendo evocare le parole dei giudici della sentenza *data retention*, di "vasta portata" e "particolarmente grave". La Corte come già affermato nella sentenza *Digital Rights Ireland*, può giustificare una deroga tanto rilevante al rispetto dei diritti fondamentali alla sola condizione che sia perseguito un obiettivo di importanza equivalente, come può essere la lotta al terrorismo e alla criminalità grave, ma anche in una situazione del genere è imprescindibile la tutela del diritto alla protezione dei dati personali e alla riservatezza da una conservazione generalizzata e indifferenziata dei dati di traffico. La Corte osservò come, da un lato, la tipologia di dati in questione fossero capaci di tracciare nel loro insieme, un profilo molto dettagliato della vita privata degli interessati, anche in relazione ad aspetti "sensibili"; dall'altro lato,

[253] Si ricorda qui che i criteri per il quale è possibile una limitazione dei diritti e delle libertà fondamentali sono ex art. 52 della Carta di Nizza sono: 1) una previsione di legge e il rispetto del suo contenuto essenziale; 2) il rispetto del principio di proporzionalità; 3) il perseguimento di scopi di interesse generale.

[254] O. POLLICINO – M. BASSINI, *LA CORTE DI GIUSTIZIA …*, cit., p. 6.

come le misure previste dalla normativa nazionale non lasciassero spazio ad alcuna differenziazione, limitazione o eccezione rispetto ai soggetti sospettati o coinvolti e all'obiettivo perseguito, riguardando in modo invasivo tutti gli individui destinati ad avvalersi di servizi di comunicazione elettronica, non essendo prevista nessuna correlazione tra i dati di cui si richiedeva la conservazione e l'esistenza di una minaccia per la sicurezza pubblica. Tantomeno non era prevista alcuna notificazione agli interessati, ingenerando in tal modo la sensazione di una sorveglianza costante, e nessun tipo di limitazione in relazione al periodo di tempo, all'ambito geografico o alla cerchia di individui cui sarebbe stata indistintamente applicabile la conservazione dei dati di traffico.

Tutti questi elementi fecero sì che la Corte dichiarasse la normativa svedese eccedente i limiti dello "stretto necessario", di conseguenza non trovando giustificazione nell'articolo 15 della direttiva 2002/58/CE.

In merito alla seconda questione pregiudiziale sollevata dal giudice britannico a nome dei signori Tom Watson, Peter Brice e Geoffrey Lewis nei confronti *Secretary of State for the Home Department*, la Corte esaminò la compatibilità con il diritto dell'Unione, della disposizione del *Data Retention and Investigatory Powers Act* 2014 (DRIPA) per cui era consentito al Ministero dell'Interno britannico di imporre ai fornitori di servizi di comunicazione elettronica la conservazione dei dati senza alcun preventivo scrutinio delle autorità competenti.

La Corte anzitutto fece riferimento al carattere tassativo dell'elenco indicato dall'articolo 15, par. 2, della direttiva del 2002, sottolineando come solo il perseguimento di uno degli obiettivi considerati nella suddetta disposizione, fosse giustificabile in termini di ingerenza nei diritti di cui agli articoli 7 e 8 della Carta di Nizza.

In seconda battuta, la Corte si soffermò sul principio di proporzionalità, argomentando che, nel rispetto degli obiettivi previsti dall'articolo 15, l'accesso ai dati garantito alle autorità nazionali competenti deve avvenire entro i limiti dello stretto necessario, in presenza di norme chiare e precise che ne identifichino

i presupposti[255]. A tal fine secondo la Corte di Giustizia era necessaria la predisposizione di criteri oggettivi all'interno della normativa nazionale ad esempio circoscrivendo l'accesso ai dati per la lotta alla criminalità e al terrorismo solo alla cerchia di persone sospettate di progettare, commettere o aver commesso una grave violazione o reato. Si richiese, inoltre, salvo i casi di urgenza, che l'accesso fosse sottoposto a un controllo preventivo di un organo giurisdizionale o amministrativo indipendente, o ancora che gli interessati fossero informati dell'adozione di tali misure da parte dell'autorità procedente una volta che le indagini non potessero essere più compromesse dalla comunicazione.

In conclusione, per la Corte, ogni misura volta alla conservazione dei dati di traffico ordinata dalle autorità nazionali poteva trovare giustificazione nel diritto dell'Unione e non configurava una violazione dei diritti fondamentali di cui gli artt. 7, 8 e 11 della Carta, solamente laddove fossero rispettate le condizioni ora descritte che consentivano di limitarne entro i limiti di stretta necessità l'applicazione.

4. Il Bundesverfassungsgericht e la recente sentenza sui c.d. captatori informatici: tra istanze di rafforzamento delle indagini di prevenzione al terrorismo e la difesa del "diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici"

Il Tribunale costituzionale federale tedesco con la sentenza del 20 aprile 2016[256] è tornata per la seconda volta sul tema della sorveglianza occulta e degli strumenti che permettono la captazione di informazioni da remoto, dichiarando l'incostituzionalità di alcune disposizioni della legge federale denominata "*Bundeskriminalamtgesetz"* (BKAG), che disciplina i compiti e l'attività della

[255] *Ibidem*, p. 8.

[256] BUNDESVERFASSUNGSGERICHT**,** I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09. Per un primo commento si veda A. VENEGONI – L. GIORDANO, La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici, in Diritto penale contemporaneo, 2016.

forza di polizia federale, il "*Bundeskriminalamt"* (BKA), e la cooperazione in materia penale tra i Governi statali e quello federale e con i Paesi terzi. Si tratta, in particolare, di disposizioni indirizzate al rafforzamento delle misure di prevenzione delle minacce terroristiche internazionali.

Bisogna comunque sottolineare che non è la prima volta che il Tribunale Costituzionale tedesco si pronuncia su questa tematica. Infatti il 27 febbraio del 2008 il BVerfG[257], in una decisione che ha avuto ampia notorietà, censurò l'art. 5, comma secondo, n. 11 della legge sulla protezione della Costituzione del Nord Reno-Westfalia, perché consentiva ad un organismo di intelligence governativa il monitoraggio e l'accesso segreto a qualsiasi sistema informatico collegato in rete, permettendo ai servizi segreti del Nord Reno-Westfalia di cercare e di intercettare in modo occulto comunicazioni via internet. Bisogna chiarire che il Tribunale costituzionale non censurò in toto lo strumento di indagine, riconoscendone in astratto l'ammissibilità. La ragione alla base della censura fu l'insufficienza delle garanzie costituzionali a tutela della segretezza delle comunicazioni e dell'inviolabilità del domicilio. La sentenza del Bundesverfassungsgericht acquisì notevole importanza specialmente perché, per la prima volta nel panorama giuridico europeo, veniva riconosciuta l'esistenza di un nuovo diritto costituzionale: il *"diritto fondamentale alla garanzia dell'integrità e della riservatezza dei sistemi informatici"*, corollario del più generale *"diritto alla dignità"*. Secondo quanto riportato dai giudici del BVerfG il nuovo diritto «*protegge la vita personale e privata dei titolari dei diritti dall'accesso statale a dispositivi tecnologici di informazione, in particolare dall'accesso da parte dello Stato ai sistemi tecnologici di informazione nel loro complesso, non solo dunque per eventi di comunicazione individuale o memorizzazione dei dati*». Il Tribunale costituzionale tedesco fa discendere da questa nuova posizione di diritto una legittima aspettativa alla riservatezza per gli utenti tanto dei loro dati, quanto dei sistemi informatici di

[257] Sentenza del Bundesverfassungsgericht del 27 febbraio 2008, 1 BVR 370/97 sulla c.d. *online durchsuchung*, con nota di R. FLOR, *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung,* in *Riv. trim. dir. pen. econ*., 3, 2009.

riferimento. Si determinava nel caso di specie una ingerenza ingiustificata, basata su una netta sproporzione tra mezzi utilizzati e gli scopi perseguiti. Il BVerfG ribadì allora il principio per cui il ricorso a nuove forme di investigazione tecnologica implicava necessariamente un bilanciamento, da compiere a livello legislativo, con eventuali interessi contrapposti, a partire dai diritti fondamentali dell'individuo.

Per quel che qui interessa, relativamente all'utilizzo di nuove tecnologie al fine di migliorare i mezzi di indagine per la lotta al terrorismo, ma che al contempo sono capaci di comportare gravi ingerenze nei diritti fondamentali delle persone, la sentenza del 20 aprile 2016 ha premesso che è compito del legislatore trovare un equilibrio tra il dovere dello Stato di proteggere la popolazione da gravi minacce e la garanzia dei diritti fondamentali. Il BVerfG individuò i due termini del bilanciamento evidenziando come da una parte i mezzi efficaci di raccolta di informazioni fossero di grande importanza per la protezione contro le minacce all'ordine democratico e agli stessi diritti fondamentali provenienti dal terrorismo internazionale, e dall'altra parte come il potere della polizia federale di raccogliere segretamente dati personali consentisse gravi interferenze nella vita privata e nel domicilio, la cui protezione è centrale per la salvaguardia della dignità umana[258].

Di conseguenza era imprescindibile un attento scrutinio sotto la lente d'ingrandimento del principio di proporzionalità da parte del BVerfG.

Dal principio di proporzionalità il tribunale costituzionale tedesco fece discendere alcuni principi base prevedendo che:

a) la raccolta segreta di dati personali può estendersi dalla persona oggetto dell'indagine a terzi estranei solo a determinate condizioni particolari;
b) il nucleo della vita privata deve essere rigorosamente preservato per mezzo di norme particolari che innalzano il livello di garanzia;

[258] A. VENEGONI – L. GIORDANO, La Corte Costituzionale tedesca sulle misure di sorveglianza occulta…, cit., punto 2.

c) le persone che sono soggette al segreto professionale devono essere sufficientemente tutelate;
d) l'esercizio dei poteri investigativi deve avvenire in modo trasparente e sotto il controllo giurisdizionale;
e) dopo che le misure sono state poste in essere, le parti interessate devono essere informate e poste in grado di attivare un controllo giurisdizionale;
f) la legge deve prevedere i requisiti per la cancellazione dei dati personali raccolti dopo il loro utilizzo.

Il Tribunale costituzionale tedesco prese in analisi i paragrafi dal 20a al 20x della BKAG, censurandoli sotto vari profili.

Il BVerfG in prima istanza prese in considerazione il paragrafo 20g della BKAG, relativo all'uso di mezzi speciali di sorveglianza in luoghi diversi dal domicilio, come l'osservazione, la registrazione audio-video, l'applicazione di dispositivi di localizzazione o l'uso di informatori della polizia, ritenendo che i poteri riservati alla polizia federale fossero troppo estesi. Ciò in particolare perché anzitutto mancava all'interno della disposizione una limitazione all'utilizzo di tali strumenti incentrata sulla prevedibilità in concreto di uno specifico fatto-reato, violando in maniera aperta il principio di proporzionalità e rendendo arduo un controllo a posteriori. Inoltre la disposizione non prendeva in considerazione l'adozione di misure per garantire il rispetto di uno spazio "assolutamente riservato" precluso nel modo più assoluto all'ingerenza pubblica; mentre per quanto riguardava il monitoraggio a lungo termine o per l'ascolto di conversazioni non pubbliche le disposizioni erano poco chiare sul quando fosse necessaria un'autorizzazione giudiziaria.

Particolarmente importante era la determinazione di cui al paragrafo 20k della BKAG. In questo punto il BVerfG determinò che l'utilizzo di strumenti capaci di accedere ai sistemi informatici da remoto, veicolati sottoforma di virus (trojan) tramite l'invio di mail, messaggi o il download di applicazioni sul sistema che si vuole sorvegliare, non assicuravano una protezione sufficiente del nucleo profondo della vita privata. La principale critica mossa a riguardo, oltre alla

particolare invasività di tali strumenti, consisterebbe nel fatto che fosse previsto un controllo ad opera del personale dell'ufficio federale di polizia penale e non di soggetti esterni e indipendenti.

Il Tribunale Costituzionale tedesco infine, per tutti i poteri d'indagine e di sorveglianza ravvisava la mancanza di talune disposizioni supplementari necessarie ad assicurare il rispetto dei limiti costituzionali come ad esempio la previsione di una tutela per le persone che possano avvalersi del segreto professionale (in modo specifico degli avvocati), o la previsione di disposizioni che mirano a garantire la trasparenza dei procedimenti, mancavano specificazioni adeguate sulla revisione obbligatoria delle misure sugli obblighi d'informazione nei confronti del Parlamento e del pubblico e infine la previsione relativa alla cancellazione dei dati raccolti era insufficiente, in particolare, perché il paragrafo 20v del BKAG rendeva possibile la memorizzazione di dati in vista di nuovi usi per la prevenzione dei reati o come precauzione per il perseguimento futuro di un reato di notevole rilevanza[259]. Il ruolo del Bundesverfassungsgericht nelle due sentenze citate, e quello della Corte di Giustizia europea è stato fondamentale al fine di riequilibrare i principi in tema di mezzi di contrasto a forme di gravi criminalità e di terrorismo e diritti fondamentali. A seguito delle sempre più frequenti minacce terroristiche, l'occhio delle Corti, nazionali e sovranazionali, deve essere ancora più vigile al fine di evitare che la genericità delle legislazioni nazionali improntate ad una tenace lotta contro il "nemico", al fine di garantirsi forse il più ampio margine d'azione possibile, non finisca con il degradare e svilire la ragione per cui vale la pena lottare così assiduamente, e cioè i diritti fondamentali dell'uomo.

[259] *Ibidem*, punto 3.4.

5. La Corte di Cassazione Italiana sui captatori informatici da remoto (trojan): un significativo cambio di rotta

A conferma del fatto che la tematica del rapporto tra rafforzamento dei mezzi investigativi per la lotta a gravi reati, quali il terrorismo, e garanzie fondamentali della persona sta assumendo, all'interno di ogni ordinamento europeo una posizione centrale nel dibattito politico e giurisprudenziale, quasi contemporaneamente alla sentenza tedesca, la Corte di Cassazione a Sezioni Unite ha avuto modo di pronunciarsi sull'utilizzo del sistema di captazione delle conversazioni tra privati attraverso sistemi informatici portatili[260].

La Corte di Cassazione con un pronuncia "controcorrente" arriva ad affermare la compatibilità dell'utilizzo dei captatori informatici da remoto, nello specifico dei software *trojan*, per i delitti di criminalità organizzata, nelle intercettazioni tra presenti anche senza previa indicazione dei luoghi dove quest'ultime devono svolgersi.

L'intercettazione tramite captazione da remoto è un mezzo di sorveglianza estremamente efficiente e molto difficile da scoprire. I c.d. software trojan possono insinuarsi facilmente all'interno dei sistemi informatici, tramite l'invio di una mail, un sms, un download di un'applicazione o tramite una chiavetta usb, e sono capaci di attivare a distanza dispositivi che generalmente i soggetti intercettati portano con loro in tutti i loro spostamenti (smartphone, tablet, computer portatile, Apple watch...), rendendo la capacità di intercettazione molto maggiore ed efficace. Questi captatori infatti consentono una gamma molto ampia di operazioni intrusive, che comprendono: l'accesso (con facoltà di copia) ai dati memorizzati nel dispositivo, la registrazione del traffico dati in arrivo o in partenza (incluso quanto digitato sulla tastiera), la registrazione delle telefonate e

[260] CORTE DI CASSAZIONE, Penale, Sezioni Unite, sentenza n. 26889, 1 luglio 2016. Per dei primi commenti si veda M. T. ABBAGNALE, *In tema di captatore informatico,* in *Archivio penale*, n. 2/2016 e G. LASAGNI, *L'uso di captatori informatici (Trojans) nelle intercettazioni "fra presenti"*, in *Diritto penale contemporaneo*, 2016. Si veda inoltre M. RUBECHI, *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it* n. 23/2016.

delle videochiamate e, soprattutto, l'attivazione delle funzioni microfono e/o telecamera indipendentemente dalla volontà dell'utente[261].

Il ricorso alle Sezioni Unite nasce da un'ordinanza di conferma di una misura di custodia cautelare emessa dal Tribunale di Palermo, nei confronti di un soggetto accusato di partecipare all'associazione mafiosa "Cosa Nostra", al quale erano stati applicati metodi di sorveglianza e di intercettazione tramite captatori informatici da remoto. L'ordinanza viene impugnata per vari motivi tra cui l'inutilizzabilità delle intercettazioni ex articolo 266 comma 2 c.p.p. per due diverse ragioni: prima di tutto perché non era stato rispettato il divieto di eseguire intercettazioni all'interno di abitazioni private, giacché la captazione sarebbe stata autorizzata senza che all'interno dei luoghi si stessero svolgendo attività criminose (di qui la conseguente violazione della riserva di legge prevista dall'art. 14 Cost.); poi si contestava che la captazione fosse stata disposta senza indicare precisamente dove sarebbe dovuta essere effettuata, limitandosi a indicare genericamente il luogo ove fosse «*ubicato in quel momento l'apparecchio portatile*» . Ciò avrebbe comportato la violazione non solo della norma codicistica, ma anche delle garanzie poste a tutela dei diritti fondamentali previsti dagli art. 15 Cost. e 8 CEDU. Va ricordato qui che l'indicazione dei luoghi come requisito di legittimità delle intercettazioni ex art. 266, co. 2, del c.p.p. era ripresa da una sentenza della stessa Cassazione in un caso analogo del 2015 (n. 27100, Musumeci). In tale pronuncia la Sesta Sezione di Cassazione aveva infatti affermato che la formulazione dell'art. 266, comma 2 c.p.p. implicherebbe l'obbligo di specificare, nel decreto di autorizzazione, il luogo in cui le captazioni devono svolgersi, ritenendo che l'uso di uno strumento di *surveillance,* capace di seguire il soggetto in qualunque luogo esso si trovi, risulterebbe, quindi, sempre illegittimo per violazione della libertà e della segretezza delle comunicazioni[262]. Sul ricorso dell'indagato fu adita sempre la sesta Sezione, la quale optando per un cambio di interpretazione rispetto alla

[261]G. LASAGNI, *ibidem.*
[262] *Ibidem,* p. 4.

sentenza del 2015, rimise la questione alle Sezioni Unite. La Sesta Sezione sottolineava come nonostante l'incompatibilità tra l'utilizzo dei trojan e la possibilità di prestabilire i luoghi in cui la captazione dovesse essere effettuata, non sussistesse alcuna base legale, desumibile né dalla legge, né da altra giurisprudenza a livello nazionale o sovranazionale, per imporre quest'ultimo requisito ai fini della legittimità del mezzo di ricerca della prova. Allo stesso modo l'indicazione del luogo come requisito essenziale, emergerebbe solo nel caso in cui l'operazione di captazione dovesse avvenire in abitazioni o luoghi privati, restrizione che, tuttavia, non opera per i procedimenti di "criminalità organizzata" per cui vige la disciplina derogatoria speciale prevista dall'art. 13 d.l. 13 maggio 1991, n. 152 (convertito nella legge 12 luglio 1991, n. 203). In ogni caso, si sosteneva che la mancanza dell'indicazione del luogo dell'intercettazione potesse comunque essere compensata da un controllo postumo sull'utilizzabilità del materiale raccolto da effettuarsi, ad esempio, durante l'udienza "stralcio" di cui all'art. 268 comma 6 c.p.p.

Il punto di vera svolta del ragionamento ermeneutico delle Sezioni Unite, che accoglie il cambio di orientamento proposto dalla Sesta Sezione, risiede nel concetto di intercettazione "ambientale" e "fra presenti". Innanzitutto, la Cassazione chiarisce come il termine "intercettazione ambientale" non abbia riscontro in nessun testo normativo, nemmeno nello stesso art. 266 comma 2 c.p.p., dove si parla invece di intercettazione di "comunicazioni fra presenti". Un riferimento ad un preciso contesto ambientale è previsto solo nella seconda parte del secondo comma dell'art. 266, quando si parla di privata dimora[263]. La necessità di indicare con precisione e a pena di inutilizzabilità i luoghi nei quali le intercettazioni tra presenti devono essere effettuate non trova riscontro nemmeno nella giurisprudenza di legittimità che, fino alla sentenza Musumeci del 2015, non aveva mai richiesto tale elemento per ambienti diversi dalla privata

[263] In tal senso, ad esempio, Cass., Sez. I, sent. 25 febbraio 2009, dep. 16 marzo 2009, n. 11506, secondo cui: «*La intercettazione di comunicazioni tra presenti richiede – per come si desume chiaramente dal tenore dell'art. 266, secondo comma ult. parte C.P.P. – la indicazione dell'ambiente nel quale la operazione deve avvenire solo quando si tratti di abitazioni o luoghi privati, secondo l'indizione di cui all'art. 614 del codice penale*».

dimora. Afferma la Corte che l'indicazione preventiva del luogo ha rilevanza esclusivamente quando vi sia «*fondato motivo di ritenere che ivi si stia svolgendo l'attività criminosa*». Sarebbe dunque privo di alcuna effettiva base legale, concludono le Sezioni unite, l'obbligo di previsione del luogo come requisito sempre necessario per la legittimità delle intercettazioni. Da ciò, dopo l'analisi anche della giurisprudenza della Corte EDU che ugualmente in tema di intercettazioni non prevede l'indicazione del luogo come requisito di legittimità dell'intercettazione[264], i giudici di legittimità concludono che la locuzione "ambientale" non costituisce un parametro normativo, ma esclusivamente un termine ampiamente diffuso in dottrina, giurisprudenza e nel linguaggio comune, che rileva tra l'altro punti di coincidenza con l'intercettazione "fra presenti"(cioè al di fuori del mezzo telefonico). Da tale assimilazione la Corte fa discendere l'impossibilità di determinare a priori l'illegittimità delle intercettazioni svolte con dispositivi di captazione "itineranti", in grado di seguire il soggetto ovunque esso si trovi, anche se incapaci di interrompere la registrazione in base al luogo in cui sono posti.

Le Sezioni Unite inoltre rilevano come nella sentenza Musumeci non si sia presa in considerazione la normativa speciale predisposta dall'art. 13 d.l. 152/1991, secondo il quale l'intercettazione all'interno del domicilio disposta «*in relazione ad un delitto di criminalità organizzata*» è consentita «*anche se non vi è motivo di ritenere che nei luoghi predetti si stia svolgendo l'attività criminosa*» e consentendo esplicitamente allo Stato di utilizzare «*tutti i mezzi che la moderna tecnologia offre*». In questo specifico caso il legislatore ha optato per un bilanciamento più rigido degli interessi in gioco, accondiscendendo ad una più pregnante limitazione delle garanzie costituzionali, ma solo in relazione alla eccezionale gravità e pericolosità delle minacce che pervengono dalle organizzazioni criminali a danno della società e dei singoli.

[264] Si veda CORTE EDU, *Zakharov c. Russia*, ricorso n. 47143/06, 4 dicembre 2015, § 227 ss. e CORTE EDU, *Capriotti c. Italia*, ricorso n. 28819/12, 23 febbraio 2016, § 43- 44.

Di conseguenza, nel caso di specie, a maggior ragione del fatto che il ricorrente fosse un appartenente ad un'organizzazione criminale di stampo mafioso, la Corte di Cassazione a Sezioni unite conferma che l'indicazione del luogo non può essere considerata elemento necessario del decreto di autorizzazione delle intercettazioni e, nel caso si persegua un delitto di criminalità organizzata, nemmeno quando queste debbano svolgersi all'interno del privato domicilio (ex art. 13 d.l. 152/1991).

Sotto il profilo della legittimità dell'utilizzo di questi nuovi strumenti tecnologici ai fini d'indagine, la pronuncia delle Sezioni unite sembra abbracciare il principio di "neutralità tecnica", principio già riconosciuto in tema di protezione dei dati personali, secondo cui la normativa dovrebbe trovare applicazione a prescindere dalla tecnologia utilizzata per ottenere un determinato scopo. Neutralità tecnica che non deve comunque essere intesa come un'impropria e pericolosa legittimazione in via giurisprudenziale di qualsiasi mezzo di indagine, anche se altamente intrusivo[265]. La Direttiva UE 2016/680 in tema di protezione dei dati personali con riferimento ad attività quali la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali, prende infatti esplicitamente in considerazione le sfide poste dalla rapidità dell'evoluzione tecnologica e dalla globalizzazione, ed evidenzia come «*al fine di evitare che si corrano gravi rischi di elusione, la protezione delle persone fisiche dovrebbe essere neutrale sotto il profilo tecnologico e non dovrebbe dipendere dalle tecniche impiegate*[266]». Secondo il parere di autorevole dottrina allora «*sarebbe quindi auspicabile un intervento legislativo che identificasse chiaramente non tanto tutte le singole tecnologie utilizzabili nel campo delle intercettazioni (che prima erano microspie, oggi sono virus informatici, ma potrebbero ovviamente a breve avere anche forma ben diversa), quanto piuttosto le garanzie fondamentali che devono sempre essere riconosciute all'indagato e*

[265] G. LASAGNI, *L'uso di captatori informatici…*, cit., p. 11.
[266] Cfr. Considerando n. 18, Direttiva 2016/680.

ai soggetti terzi potenzialmente coinvolti, a prescindere dallo strumento utilizzato».

In ogni caso con la sentenza in esame le Sezioni Unite rigettano il ricorso dell'indagato, confermando la corrente interpretativa inaugurata dalla Sezione rimettente a discapito di quanto affermato nel 2015 nel caso Musumeci. Così facendo i giudici di legittimità, intervengono sul contrasto interpretativo fra due diversi orientamenti espressi dalla stessa Sezione VI a poco meno di un anno di distanza fra loro. Contemporaneamente alla ricostruzione della disciplina dei presupposti per le intercettazioni "fra presenti" la Corte di Cassazione avalla ufficialmente l'ingresso, nel nostro ordinamento, dei captatori informatici "polivalenti" come strumenti di indagine penale.

CONCLUSIONI

L'introduzione del Regolamento UE 2016/679 è stato da tempo auspicato e accolto in un generale sentimento di ottimismo. Da molti l'introduzione di una disciplina generale, mediante l'adozione di un atto vincolante e *self executing*, è sembrata la risposta adeguata alle dinamiche del nostro tempo, scandito dalla vertiginosa evoluzione e rivoluzione del contesto in cui il diritto alla protezione dei dati personali opera.

Se per alcuni l'estrema vocazione al dettaglio, nell'individuare una disciplina puntuale e il più possibile onnicomprensiva, porta con sé il rischio di un rapido invecchiamento, per altri l'ampliamento dei poteri delle Autorità garanti da una parte, e la previsione di specifici e rigorosi obblighi in capo ai soggetti che pongono in essere il trattamento dei dati personali (*Controller e Processor*), specialmente nell'ambito delle misure di sicurezza da adottare, dall'altra parte possono rappresentare un'efficace garanzia di un'evoluzione interpretativa proiettata verso il futuro, ma saldamente ancorata ai principi fondanti la materia.

In ogni caso il Regolamento n. 679 del 2016 sembra fornire «*risposte puntuali a problemi puntuali*», individuando i problemi e le principali lacune del passato e cercando di fornire strumenti che garantiscano un elevato livello di protezione.

Lodevole, a parere di chi scrive, il netto cambio di prospettiva dell'intera disciplina improntata, ora, nella concentrazione massima alla prevenzione del danno e delle lesioni ai diritti fondamentali che potrebbero derivare da una violazione delle misure di sicurezza o da un trattamento illegittimo.

Ciò soprattutto, in base alla definizione dell'attività di trattamento dei dati personali come un'attività pericolosa. Così facendo è previsto un obbligo generale da parte dei titolari e dei responsabili del procedimento di mettere «*in atto misure tecniche e organizzative adeguate per garantire (...) che il trattamento è effettuato conformemente al presente regolamento*», al fine di evitare la responsabilità e il gravoso regime sanzionatorio che ne consegue.

Tale impostazione preventiva-precauzionale del nuovo sistema di tutela si coglie espressamente nell'introduzione di particolari istituti come la valutazione pre-impatto, da attuare quando vi sia il timore che il trattamento comporti «*un elevato rischio per i diritti e le libertà delle persone fisiche*»; oppure come la consultazione preventiva da richiedere all'autorità garante nazionale nel caso in cui all'esito della valutazione d'impatto risulti necessario un parere specifico; o ancora per mezzo dell'introduzione dei principi di protezione fin dalla progettazione (*by design*) e per impostazione predefinita (*by default*) grazie ai quali è possibile elaborare tutte le misure necessarie alla protezione dei dati ancor prima di porre in essere il trattamento e, al contempo, garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.

Il Regolamento, a differenza della precedente normativa, pone al centro della "nuova protezione" dei dati personali il trattamento e le misure di sicurezza, la cui conformità ai principi del Regolamento, è intesa quale presupposto essenziale della tutela e dell'esercizio dei diritti degli interessati.

Il Regolamento inoltre, ribadisce e rafforza punti fermi delle discipline previgenti tra cui il ruolo centrale del consenso, affiancato dai doveri di informazione e trasparenza, il sistema generale dei principi e delle definizioni, aggiornandolo e riadattandolo all'esigenze del panorama odierno.

Introduce nuove figure, destinate ad avere senza dubbio un grande impatto all'interno dello scenario della protezione dei dati personali, come per quanto riguarda il *Data protection officer*: una figura specializzata e dotata del carattere di professionalità e autonomia che ha il compito di coadiuvare il titolare del trattamento durante l'espletamento dei suoi compiti, ma che allo stesso tempo risulta essere un punto di riferimento e di collegamento sia per le autorità garanti nazionali, sia per gli stessi soggetti interessati.

Inoltre il Regolamento, saggiamente, alterna definizioni e concetti dotati di particolare genericità ad altri dotati di maggiore precisione, evidenziando che

poche materie come questa «*necessitano di un difficile mix tra definizioni legislative elastiche e, ove occorra, di interventi regolamentari di dettaglio*».

Infine, la nuova disciplina sembra aver fatto tesoro di tutte le determinazioni, spesso a dir poco "pioneristiche", elaborate dalla Giurisprudenza negli ultimi vent'anni e dalla instancabile opera esegetica dei Garanti nazionali e del Gruppo di Lavoro comune ex articolo 29.

Si pensi solamente alla declinazione del diritto all'oblio come diritto alla de-indicizzazione di un risultato, prodotto per mezzo di un motore di ricerca, di una determinata pagina web come sancito nella sentenza *Google Spain*, o ancora si pensi alla riforma della disciplina relativa al trasferimento dei dati verso Paesi terzi come scardinata dalla sentenza *Schrems*.

In considerazione di tutto ciò può affermarsi che il Regolamento UE 2016/679 rappresenta sicuramente un grande passo avanti nel panorama giuridico della protezione dei dati personali, non solo per le novità introdotte, che risultano senz'altro particolarmente significative, ma soprattutto per il rafforzamento e la conferma dei principi e delle determinazioni contenute nelle normative precedenti. Una nuova disciplina che affonda le sue radici nel passato (in particolare nella Direttiva 95/46/CE), ma fortemente proiettata verso il futuro.

Sicuramente grazie alla "veste" mediante il quale questa nuova disciplina è introdotta (quella del regolamento ai sensi dell'art. 288 TFUE, e perciò generale, vincolante e direttamente applicabile) sembra più facilmente raggiungibile, ora più di prima, l'obiettivo del legislatore comunitario di elevare il grado di armonizzazione ed eliminare le discrepanze, evidenziatesi in questi anni, tra le varie normative nazionali, predisponendo un sistema uniforme e coordinato su tutto il territorio UE in materia di protezione dei dati personali.

Per quanto riguarda invece l'ambito della cooperazione giudiziari e di polizia, sicuramente apprezzabile risulta lo sforzo, da parte della Direttiva UE 2016/680, di introdurre anche in questo settore i principi e parte delle novità enucleate nel nuovo Regolamento, al fine di predisporre, anche qui, la massima protezione possibile.

Operazione in parte riuscita, grazie anche ad un'analisi dei limiti e dei difetti dei precedenti strumenti legislativi e la conseguente introduzione di strumenti più efficienti in direzione di un auspicato equilibrio tra tutela dei dati personali e lotta alla criminalità e al terrorismo (si pensi ad esempio al rafforzamento del principio di disponibilità, delle misure di sicurezza e degli obblighi del titolare, alla necessaria verifica della qualità dei dati come presupposto alla trasmissione degli stessi, alla codificazione, anche qui, dei principi della *privacy by design and default* o della valutazione pre-impatto e della consultazione preventiva, e infine all'estensione della disciplina al trattamento domestico, prima escluso).

È pur vero che forse scelte più audaci e ambiziose non si potevano pretendere in un settore che negli ultimi anni è stato fortemente scosso dall'emergenza terroristica e che tradizionalmente è oggetto di "geloso" dominio dei singoli Stati.

È infatti vero che in circostanze storiche in cui episodi di terrorismo mettono a repentaglio la vita dei cittadini e le principali istituzioni democratiche, il sentimento della popolazione tende verso la richiesta di rigide misure di prevenzione e di polizia, considerando favorevolmente il potenziamento degli strumenti di controllo, anche se a discapito di posizioni di diritto consolidate.

Anche in queste situazioni però un ordinamento democratico non può mai scendere a patti con la compressione eccessiva dei diritti fondamentali riconosciuti ai cittadini, in ossequio alla salvaguardia della dignità umana e delle libertà.

È chiaro che il nostro ordinamento può tollerare limitazioni ai diritti fondamentali, specialmente se al fine di proteggere l'incolumità della popolazione da gravi minacce, ma è necessario sempre individuare la proporzionalità e la ragionevolezza delle misure adoperate dalle autorità competenti di sicurezza rispetto ai diritti fondamentali, evitando che la compressione non superi il "legittimamente tollerabile".

A tal proposito, importantissima è stata l'opera giurisprudenziale della Corte di Giustizia europea e delle Corti nazionali che, caso per caso, hanno concorso

all'elaborazione di parametri chiave della protezione dei dati personali, all'interno del settore di cooperazione giudiziaria e di polizia, ma soprattutto sono state l'ago della bilancia nel ripristino dell'equilibrio tra istanze di protezione dei dati personali ed esigenze di sicurezza nazionale, spesso fortemente sbilanciate a favore di quest'ultime a causa dell'emanazione di legislazioni emergenziali statali, più marcatamente orientate ad un potenziamento degli strumenti di controllo e prevenzione.

In ogni caso, il diritto alla protezione dei dati personali nello specifico e il diritto alla *privacy* in generale, nonostante le paure, le incertezze e le sfide poste dal terrorismo islamico di nuova generazione, non hanno smesso di estendere la loro portata contenutistica e, grazie specialmente al supporto delle Corti sovranazionali, hanno dimostrato di avere gli "anticorpi" necessari per proteggere il nucleo essenziale dei diritti fondamentali.

In conclusione, al di là dell'entusiasmo per una riforma di così ampia portata e significato, non resta che aspettare con trepidante attesa e ottimismo, quella che sarà l'attuazione concreta del nuovo "Pacchetto della protezione dati", e capire se in risposta alle dinamiche e alle sfide del *web 2.0* si possa rispondere con un diritto alla protezione dei dati personali di seconda generazione, un *right to data protection 2.0*.

Bibliografia:

ABBAGNALE M. T., *In tema di captatore informatico,* in *Archivio penale*, n. 2/2016;

BIFULCO R., *La sentenza Schrems e la costruzione del diritto europea alla privacy*, in *Giurisprudenza Costituzionale*, Anno LXI Fasc. 1, Milano, 2016;

BLACK E., *L'IBM e l'olocausto. I rapporti fra il Terzo Reich e una grande azienda americana*, Rizzoli, 2001;

BONINI M., *Sicurezza e tecnologia, fra libertà negative e principi liberali. Apple, Schrems e Microsoft: dei diritti" violabili" in nome della lotta al terrorismo e ad altri pericoli, nell'esperienza statunitense ed europea*, in *Rivista AIC*, 2016;

CAGGIANO G., *Attività di stabilimento e trattamento dei dati personali,* in *Dir.inf.*, 2014;

CALVANO R., *Chi è la più bella del reame? Corte di Giustizia e Corte di Strasburgo alla luce del parere2/13 sull'adesione alla CEDU*, in Diritto Pubblico Europeo Rassegna online, 2015;

CANNAVICCI M., *Terrorismo e intelligence,* Cap. XXIII, in Anatomia del crimine in Italia: manuale di criminologia a cura di B. ZOLI, R. S. DE LUCA, C. MACRÌ, Milano Ed. 2016;

CAROTTI B., *Il caso Schrems, del conflitto tra riservatezza e sorveglianza di massa – il commento*, in *Giornale Dir. Amm.*, 2016;

CIAMPI S., *Principio di disponibilità e protezione dei dati personali nel "terzo pilastro" dell'Unione europea*, in AA. VV., *Cooperazione informativa*, a cura di F. Peroni -M. Gialuz,Trieste, 2009;

COMMISSIONE EUROPEA, *Salvaguardare la privacy in un mondo interconnesso – Un quadro europeo della protezione dei dati per il XXI secolo,* COM (2012), 25 gennaio 2012;

D'ANTONIO V.,"The right to tell people what they do not want to hear": *i moderni confini del diritto di fare informazione,* 2009;

D'ANTONIO – S. VIGLIAR, *Studi di diritto della comunicazione. Persone, società e tecnologie dell'informazione*, Padova, 2009;

D'ANTONIO V., "Oltre la cancellazione dei dati personali: l'originaria concezione del diritto all'oblio *offline*", *Oblio e cancellazione dei dati nel diritto europeo,* Cap. X, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

DE MINICO G., *Internet and fundamental rights in time of terrorism*, in Rivista AIC n. 4/2015;

D'ORAZIO R., *Protezione dati by default e by design*, Cap. V, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

DI GENIO G.,*Trasparenza e Accesso ai dati personali*, Cap. VIII, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

FINOCCHIARO G., *Identità personale su Internet: il diritto alla contestualizzazione dell'informazione*, in *Dir. Inf.*, 2012;

FINOCCHIARO G., *Il diritto all'oblio nel quadro dei diritti della personalità,* in *Diritto dell'Informazione e dell'Informatica*, Giuffrè, Milano, 2014;

FLOR R., *Brevi riflessioni a margine della sentenza del Bundesverfassungsgericht sulla c.d. online durchsuchung,* in *Riv. trim. dir. pen. econ*., 3, 2009;

FLOR R., *Dalla "Data retention" al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della corte di giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive "de jure condendo",* in *Il diritto all'oblio su Internet dopo la sentenza Google Spain,* RESTA G. – ZENO-ZENOVICH V., Roma, 2015

INTERNATIONAL JOURNAL, *Sicurezza , terrorismo e società*, Italian Team for Security, Terroristic Issues & Managing Emergencies, 2016;

LA PISCOPIA S., *Strumenti di lotta al terrorismo internazionale. Dall'indagine tradizionale "post delictum" alle frontiere della "proactive investigation"*, in La Giustizia Penale, 2014;

LA PISCOPIA S., *Misure investigative speciali e diritti umani tra nuove strategie internazionali e recenti normative metropolitane antiterrorismo*, in La Giustizia Penale, 2015;

LASAGNI G., *L'uso di captatori informatici (Trojans) nelle intercettazioni "fra presenti"*, in *Diritto penale contemporaneo*, 2016;

MULA D., *Trasferimento verso paesi terzi*, Cap. XIV, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

O'NEILL M., *The Evolving EU Counter-Terrorism Legal Framework*, Routledge research in EU law, Oxford, 2012;

O'NEILL M., *Terrorism and human rights- EU data protection framework,* Cap. IX, in *The Evolving EU Counter-Terrorism Legal Framework*, Routledge research in EU law, Oxford, 2012;

PACILEO P., *Il diritto alla portabilità*, Cap. XI, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

PARISI A. G., *Responsabilità e Sanzioni*, Cap. XV, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

PIZZETTI F., *Il prisma del diritto all'oblio,* in *Il caso del diritto all'oblio*, Torino, 2013;

PIZZETTI F., in *La decisione della Corte di giustizia sul caso Google Spain: più problemi che soluzioni*, 2014;

PIZZETTI F., *Privacy e il Diritto Europeo alla Protezione dei Dati Personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, Vol I de *I Diritti nella "rete" della Rete*, Torino, 2016;

POLLICINO O. – BASSINI M., *LA CORTE DI GIUSTIZIA E UNA TRAMA ORMAI NOTA: LA SENTENZA TELE2 SVERIGE SULLA CONSERVAZIONE*

DEI DATI DI TRAFFICO PER FINALITÀ DI SICUREZZA E ORDINE PUBBLICO, 2017;

RESTA G. – ZENO-ZENOVICH V., *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015;

RICCIO G. M., *Data Protection Officer e altre figure*, Cap. III, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

RODOTÀ S., *Le fonti di integrazione del contratto*, Milano, 1969;

RODOTA' S., *Tecnologie e diritti*, Bologna, 1995;

ROSSI DAL POZZO F., *La tutela dei dati personali tra esigenze di sicurezza nazionale, interessi economici e diritti fondamentali della persona (dal Safe Harbor al Privacy Shield)*, in *Rivista di diritto internazionale*, Milano, 2016;

RUBECHI M., *Sicurezza, tutela dei diritti fondamentali e privacy: nuove esigenze, vecchie questioni (a un anno dagli attacchi di Parigi)*, in *federalismi.it* n. 23/2016;

SICA S., D'ANTONIO V., RICCIO G. M., *La Nuova Disciplina Europea della Privacy*, Milano, 2016;

SICA S. – D'ANTONIO V., *La procedura di de-indicizzazione*, 2015;

STANZIONE M. G., *Genesi ed Ambito di Applicazione*, Cap. II, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

TIBERI G., *Protezione dei dati personali e sicurezza dopo il Trattato di Lisbona*, in AA. VV., *L'evoluzione del diritto penale nei settori d'interesse europeo alla luce del Trattato di Lisbona*, a cura di G. GRASSO, L. PICOTTI, R. SICURELLA, Giuffrè, Milano, 2011;

TRESCA M., *Sicurezza vs protezione dei dati: la CGUE cambia registro*, in *Amministrazione In Cammino*, 2016;

TROISI P., *La protezione dei dati trattati a fini di prevenzione e accertamento dei reati*, Cap. XVI, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;

VENEGONI A. – GIORDANO L., La Corte Costituzionale tedesca sulle misure di sorveglianza occulta e sulla captazione di conversazioni da remoto a mezzo di strumenti informatici, in Diritto penale contemporaneo, 2016;
VERIZON, *2016 Data breach Investigation Report*, 2016;
VIGLIAR S., *Data breach e sicurezza informatica*, Cap. XII, in *La Nuova Disciplina Europea della Privacy*, a cura di S. SICA, V. D'ANTONIO, G.M. RICCIO, Milano, 2016;
WARREN S.D. – BRANDEIS L.D., *The Right to Privacy*, in *Harvard Law Review*, Vol IV, Boston, n. 5, 1890;
WHITMAN J. Q., *The Two Western Cultures of Privacy: Dignity versus Liberty*, in *The Yale Law Journal*, New Haven (Connecticut), 2004;
ZENO-ZENOVICH V., *Onore e reputazione nel sistema del diritto civile*, Napoli, 1985.

Sitografia:

ALTALEX, *Decreto Anti terrorismo: il testo*, in www.altalex.com, 21 aprile 2015;
BRUGIOTTI E., *La privacy attraverso la "generazione dei diritti"*, da www.dirittifondamentali.it, Università degli studi di Cassino e del Lazio Meridionale, pdf, 2013;
CENTRO DI RICERCA E TUTELA DEI CONSUMATORI E DEGLI UTENTI, *Guida pratica agli organismi di regolazione e controllo a tutela dei consumatori*, su www.centroconsumatori.tn.it;
EUROPEAN UNION AGENCY FOR LAW ENFORCEMENT COOPERATION, Europol Information System (EIS), *A system for information on serious international crimes*, in www.europol.europa.eu;

FRA (European Union Agency for Fundamental Rights) – CONSIGLIO D'EUROPA, *Manuale sul diritto europeo in materia di protezione dei dati*, da www.fra-europa.eu, pdf, 2014;

GALGANI F., *La nascita del diritto alla privacy negli Stati Uniti e in Europa*, da www.informatica-libera.net, 2014;

GHIRIBELLI A., *Il diritto alla privacy nella Costituzione italiana*, da www.teutas.it, 2007;

GUZZO A., *Il concetto di privacy enhancing technologies*, pubb. in Sicurezza informatica e tutela della privacy, 26 febbraio 2009, reperibile all'indirizzo www.diritto.it., 2009;

IASELLI M., *I compiti del Data Protection Officer: chiariamo tutti i dubbi*, 21 aprile 2017, in www.agendadigitale.eu.;

LATTANZI R., *«Diritto alla protezione dei dati di carattere personale»: appunti di viaggio*, in *DIRITTO ALLA PRIVACY E TRATTAMENTO AUTOMATIZZATO DEI DATI FRA DIRITTO CIVILE, DIRITTO PENALE E DIRITTO INTERNAZIONALE ED EUROPEO*, da www.cde.unict.it/quadernieuropei/giuridiche/63_2014.pdf, pdf, 2014;

REMOTTI R., *Il diritto alla privacy e ricerca scientifica, Qual è il bene giuridico tutelato*, par.2, da www.web.tiscalinet.it, pdf, 2002;

VALENSISE M., *The right to be let alone*, da www.ilfoglio.it, 2010;

VARANI E., *Il "nuovo diritto" alla privacy. Dalla Carta di Nizza al "Codice in materia di protezione dei dati personali"*, da www.filodiritto.com, 2012;

ZAGREBELSKY V., *La prevista adesione dell'Unione Europea alla Convenzione europea dei diritti*, da www.europeanrights.eu, doc., 2007.

Legislazione:

CARTA DEI DIRITTI FONDAMENTALI DELL'UNIONE EUROPEA, 2000;

CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, Decreto legislativo 30 giugno 2003, n. 196;

COMMISSIONE EUROPEA, Comunicazione COM (2010) 609 del 4 novembre 2010, relativa all'esecuzione delle direttive contenute nel Piano d'azione per l'attuazione del Programma di Stoccolma;

CONSIGLIO D'EUROPA, CONVENZIONE DI STRASBURGO N.108/1981;

CONSIGLIO D'EUROPA, Comitato dei ministri (1987), Raccomandazione n. R (87) 15 agli Stati membri che disciplina l'uso dei dati personali nell'ambito della pubblica sicurezza, 17 settembre 1987;

CONVENZIONE EUROPEA DEI DIRITTI DELL'UOMO E DELLE LIBERTA' FONDAMENTALI, 1950;

COSTITUZIONE DELLA REPUBBLICA ITALIANA, 22 dicembre 1947;

COSTITUZIONE DI FRANCIA, 4 ottobre 1958;

COSTITUZIONE SPAGNOLA, 27 dicembre 1978;

LEGGE FEDERALE PER LA REPUBBLICA DI GERMANIA, 23 maggio 1949;

DECISIONE QUADRO 2002/187/GAI, Consiglio del 28 febbraio 2002 che istituisce l'Eurojust per rafforzare la lotta contro le forme gravi di criminalità, 2002 e successive modificazioni: DECISIONE QUADRO 2003/659/GAI, Consiglio del 18 giugno 2003 e DECISIONE QUADRO 2009/426/GAI, Consiglio del 16 dicembre 2008 (decisioni Eurojust);

DECISIONE QUADRO 2008/615/GAI, Consiglio del 23 giugno 2008, sul "*potenziamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo e alla criminalità transfrontaliera*", 2008;

DECISIONE QUADRO 2008/977/GAI, Consiglio del 27 novembre 2008, sulla "*protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale*",2008;

DECISIONE QUADRO 2009/371/GAI, Consiglio del 6 aprile 2009 che istituisce l'Ufficio europeo di polizia (Europol), 2009;
DIRETTIVA 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati**;**
DIRETTIVA 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro)
DIRETTIVA 2002/58/CE del Parlamento europeo e del Consiglio del 12 luglio 2002 relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche);
DIRETTIVA 2006/24/CE, 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, 15 marzo 2006;
DIRETTIVA (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, 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 e che abroga la decisione quadro 2008/977/GAI del Consiglio;
DIRETTIVA UE 2016/681 del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) dei passeggeri dei voli in arrivo o in partenza dal territorio degli Stati membri, a fini di prevenzione, accertamento, indagine e azione penale per i reati di terrorismo e altri gravi reati;
PROGRAMMA DI STOCCOLMA, *Un' Europa aperta e sicura al servizio e a tutela dei cittadini* (2010/C 115/01), 4 maggio 2010;
PARLAMENTO EUROPEO, Risoluzione 2011/2025 (INI) del 6 luglio 2011 su *Un approccio globale alla protezione dei dati personali nell'Unione europea*;

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

Giurisprudenza:

BUNDESVERFASSUNGSGERICHT, 15 dicembre 1983, Sentenza n. 209;

BUNDESVERFASSUNGSGERICHT, Sentenza del 27 febbraio 2008, 1 BVR 370/97;

BUNDESVERFASSUNGSGERICHT, I Senato, 20 aprile 2016 - 1 BVR 966/09, 1 BVR 1140/09;

CORTE COSTITUZIONALE ITALIANA, 10 dicembre 1987, Sentenza n. 479;

CORTE DI CASSAZIONE ITALIANA, Sez. I, sent. 25 febbraio 2009, dep. 16 marzo 2009, n. 11506;

CORTE DI CASSAZIONE ITALIANA, Cass. Civ., Sez. III, 5 aprile 2012, n. 5525;

CORTE DI CASSAZIONE ITALIANA, Cass. Pen., Sez. Un., sent. 28 aprile 2016 (dep. 1 luglio 2016), n. 26889;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Klass e altri c. Germania*, n. 5029/71, 6 settembre 1978;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Leander c. Svezia*, n. 9248/81, 26 marzo 1987;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Allan c. Regno Unito,* n. 48539/99, 5 novembre 2002;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Vetter c. Francia*, n. 59842/00, 31 maggio 2005;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *S. e Marper c. Regno Unito*, nn. 30562/04 e 30566/04, 4 dicembre 2008;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *B. B. c. Francia*, n. 5335/06, 17 dicembre 2009;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, Quinta sezione, Sentenza *Uzun c. Germania*, n. 35626/05, 2 settembre 2010;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, Sezione II, *Màtè Szabó e Beatrix Vissy c. Ungheria*, sentenza n. 37138/14, 13 maggio 2014;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Zakharov c. Russia*, ricorso n. 47143/06, 4 dicembre 2015;

CORTE EUROPEA DEI DIRITTI DELL'UOMO, *Capriotti c. Italia*, ricorso n. 28819/12, 23 febbraio 2016;

CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), 8 aprile 2014, *Digital Rights Ireland Ltd* (C-293/12) *contro Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung* (C-594/12) e altri, 2014;

CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), 13 maggio 2014, Sentenza nella causa C-131/12 *Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González*, 2014;

CORTE DI GIUSTIZIA EUROPEA (Grande Sezione), Sentenza nella causa C-362/14 *Maximillian Schrems vs Data Protection Commissioner*, Lussemburgo, 6 ottobre 2015;

CORTE DI GIUSTIZIA EUROPEA, (Grande Sezione), *Tele2 e Watson*, cause riunite C-203/15 e C-698/15, sentenza 21 dicembre 2016.

Garante Privacy ITA, Garante europeo della protezione dati e Gruppo di Lavoro comune Articolo 29

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI PERSONALI, Parere del 4 aprile 2007, cit. punti 61-73, e il Terzo Parere del 27 aprile 2007;

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, relativo alla proposta di decisione quadro del Consiglio sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, 27 aprile 2007;

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI, sull'iniziativa del Regno del Belgio, della Repubblica di Bulgaria, della Repubblica federale di Germania, del Regno di Spagna, della Repubblica francese, del Granducato di Lussemburgo, del Regno dei Paesi Bassi, della Repubblica d'Austria, della Repubblica di Slovenia, della Repubblica slovacca, della Repubblica italiana, della Repubblica di Finlandia, della Repubblica portoghese, della Romania e del Regno di Svezia, in vista dell'adozione di una decisione del Consiglio sul rafforzamento della cooperazione transfrontaliera, soprattutto nella lotta al terrorismo ed alla criminalità transfrontaliera, 21 luglio 2007;

GARANTE EUROPEO DELLA PROTEZIONE DEI DATI nel *Parere* 2012/ C192/ 05, del 7 marzo 2012 sul pacchetto di riforma della protezione dati;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Decisione Commissione, clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento in paesi terzi*, dir. 95-46-CE - 5 febbraio 2010;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Individuazione delle modalità semplificate per l'informativa e l'acquisizione del consenso per l'uso dei cookies*, doc. web n. 311884, 8 maggio 2014;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, *Guida al nuovo regolamento europeo in materia di protezione dati*, 2016;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI Dichiarazione sul *Rafforzamento dell'ottemperanza dei responsabili del trattamento alla normativa sulla tutela dei dati* – (WP101), Bruxelles, 2004;

GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, Parere 1/2008 (WP 148) "*sugli aspetti della protezione dei dati connessi ai motori di ricerca*", 2008;

GRUPPO DI LAVORO ARTICOLO 29 IN MATERIA DI PROTEZIONE DEI DATI PERSONALI, il Parere 8/2010 (WP 179) "*sul diritto applicabile*", 2010;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 13/2011 *sui servizi di geo-localizzazione su dispositivi mobili intelligenti*, (WP185), 16 maggio 2011;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2012 sul *Cloud computing*, (WP196), 1 luglio 2012;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 03/2014 "*sulla notifica delle violazioni dei dati personali* (WP213), 25 marzo 2014;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Parere 05/2014 "*sulle tecniche di anonimizzazione*" (WP 216), 10 aprile 2014;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Statement on the role of a risk-based approach in data protection legal frameworks* (WP 218), 30 maggio 2014;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, Lettera a Facebook sul caso Whatsapp – 27/10/2016;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee-guida sul diritto alla "portabilità dei dati"*, 13 dicembre 2016 Versione emendata e adottata il 5 aprile 2017, (WP 242), 2017;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI PERSONALI, le *Linee-guida sui responsabili della protezione dei dati (RPD)* adottate il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017), (WP 243), 2017.