Università
Ca'Foscari
Venezia

Corso di Laurea magistrale
(ordinamento ex D.M. 270/2004)
in Economia e Finanza

Tesi di Laurea

Applicazione dell'art. 35 del Regolamento UE n. 2016/679 - Data Protection Impact Assessment

Relatore:
Ch. prof. Simone MAZZONETTO

Correlatore:
Ch. prof. Enrico Maria CERVELLATI

Laureando:
Corina CHIHAI
Matricola 843121

Anno Accademico
2018-2019

Typeset by LaTeX2e

Abstract

Il presente elaborato viene focalizzato sul diritto alla privacy nel nuovo "Pacchetto protezione dati", soprattutto nel 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, obbligando l'adeguamento della normativa nazionale di ogni Stato membro entro il 24 maggio 2018.

Il GDPR *(General Data Protection Regulation)* introduce delle significative novità in tema di privacy, come ad esempio il principio dell'*accountability* (responsabilizzazione) in capo al Titolare del trattamento dati e al responsabile del trattamento dati, la figura del Responsabile Protezione Dati (RPD o DPO), il diritto alla portabilità dei dati, il diritto all'oblio, la protezione dei dati fin dalla progettazione *(Privacy by design)* e protezione per impostazione predefinita *(Privacy by Default)*, cambiando completamente la prospettiva della Direttiva 95/46/CE – la cosiddetta Direttiva "madre".

Ma il cuore dell'intera dissertazione è l'articolo 35 del GDPR, ai sensi del quale viene prevista la valutazione d'impatto sulla protezione dei dati, o la cosiddetta *Data Protection Impact Assessment (DPIA)*. Tale valutazione è un processo finalizzato a valutare il rispetto dei principi privacy – come i principi di necessità e proporzionalità – e a valutare e gestire i rischi inerenti al trattamento. In merito, si terrà conto delle Linee guida del Gruppo di Lavoro articolo 29, in special modo dei criteri per stabilire se un trattamento "possa presentare un rischio elevato" in base al Regolamento UE n. 2016/679. Al riguardo verrà sviluppato un modello di valutazione di impatto sulla protezione dei dati, nonché la sua applicazione all'interno di cinque realtà diverse, ovvero la videosorveglianza sul posto di lavoro, i dati medici in azienda ospedaliera, la richiesta del casellario giudiziario a fini assuntivi, il trattamento dei dati nel settore del telemarketing, il trattamento dei dati nell'ambito bancario.

Nota per il lettore

Typeset by LaTeX

La tesi è stata redatta con LaTeX$_{2\epsilon}$ (LaTeX home page). Esso è un programma di composizione tipografica open source e realizzato da *Leslie Lamport*, impiegando come motore tipografico TeX che fu concepito da *Donald Ervin Knuth* e distribuito negli anni '90. Al giorno d'oggi, TeX è un marchio registrato dall'*American Mathematical Society* (AMS). Il programma utilizza numerose estensioni per ampliare le sue potenzialità ed esse vengono identificate con la simbologia $\mathcal{AMS}$-LaTeX, che sta per "*LaTeX with* $\mathcal{AMS}$*'s extensions*".

L'utilizzo di LaTeXè stato integrato con delle estensioni che hanno permesso di inserire, all'interno della seguente tesi, riferimenti incrociati cliccabili. Attraverso il pacchetto, inoltre, è stato possibile produrre un indice generale, una lista delle figure e una lista delle tabelle con i relativi numeri di pagina. Con i pacchetti hyperref e url, si sono inseriti riferimenti ipertestuali come quelli utilizzati per rinviare alla *homepage* di LaTeX o alla pagina delle funzionalità sviluppate dall'*American Mathematical Society*.

Il presente lavoro mi ha, quindi, permesso di conoscere e approfondire l'uso di questo motore tipografico e far, così, comprendere al lettore le potenzialità, che qui sono solo accennate, del programma e l'impegno ad esso riservato dall'autore.

Indice

Elenco delle figure

Elenco delle tabelle

Introduzione

Il concetto di privacy ha origini antiche, tant'è vero che la sua nascita la si indentifica nei discorsi filosofici-politici fatti nelle varie *Poleis* greche. Lo stesso Aristotele faceva distinzione tra la sfera privata e la sfera pubblica, individuandone nella prima la necessità dell'uomo di creare ambienti protetti per lui e per la sua famiglia nell'intento di coltivare il bisogno di essere lasciato in pace, mentre la seconda riguardava l'attività politica a cui l'uomo era obbligato a parteciparvi attivamente.

Nel corso degli anni la nozione di privacy ha subito dei mutamenti dovuti alla continua evoluzione tecnologica, la quale ha portato all'assunzione di una connotazione giuridica della privacy, intesa come il diritto di ciascun individuo alla riservatezza. Tale significato della nozione privacy venne espressa per la prima volta da due giovani avvocati bostoniani, Samuel D. Warren (1852-1910) e Louis D. Brandeis (1856- 1941), nell'articolo *"The Right to Privacy"*, apparso il 15 dicembre 1890 sulla Harvard Law Review.

Col passare del tempo il diritto alla privacy ha acquisito sempre più spessore fino a essere considerato diritto fondamentale dell'individuo. Tale rivoluzione del diritto alla riservatezza necessaria, in special modo nel continente europeo, segnato da un quadro storico del terrore imposto dai regimi totalitari, viene registrata nel 1950 con l'adozione della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali, individuata con l'acronimo CEDU, entrata in vigore nel 1953, la quale riconosce a ciascun individuo il diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza (art.8 – CEDU).

Il progresso tecnologico, l'impiego sempre maggiore dei computer e dei registri elettronici contenenti dati personali, costituiscono dei fattori che hanno evidenziato la necessità di una normativa in merito al trattamento automatizzato dei dati personali. In risposta a tale richiesta il Comitato dei Ministri del Consiglio d'Europa ha redato la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale il 17 settembre 1980 a Strasburgo, la c.d. Convenzione n. 108, o la Convenzione di Strasburgo. Sulla stessa scia del Consiglio d'Europa anche la Comunità economica europea, il Parlamento europeo e la Commissione europea si dedicarono alla materia del-

la protezione dei dati, adottando varie Risoluzioni e Provvedimenti fino ad arrivare alla proposta di una Direttiva intenta ad armonizzare tutte le legislazioni nazionali in merito a tale materia. Si tratta della Direttiva 95/46/CE del Parlamento e del Consiglio europeo "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati", approvata il 24 ottobre del 1995, la quale vigerà per oltre un ventennio, esattamente fino al 24 maggio 2018. In sostituzione alla Direttiva 95/46/CE entra in vigore il "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", altrimenti detto "Regolamento generale sulla protezione dei dati" o "General Data Protection Regulation" (GDPR) ed è applicabile in tutti gli Stati membri dal 25 maggio 2018.

Il Regolamento Generale sulla Protezione dei Dati (GDPR), costituisce il cuore dell'intera dissertazione, di conseguenza verrà analizzato nei minimi dettagli, ponendo l'attenzione sulle novità da esso introdotte come il principio dell'*accountability* (responsabilizzazione) in capo al Titolare del trattamento dati e al responsabile del trattamento dati, la figura del Responsabile Protezione Dati (RPD o DPO), il diritto alla portabilità dei dati, il diritto all'oblio, la protezione dei dati fin dalla progettazione *(Privacy by design)* e protezione per impostazione predefinita *(Privacy by Default)*, la valutazione di impatto sulla protezione dei dati (DPIA).

Il Regolamento UE è differente dalle normative precedenti in materia di protezione dei dati, in special modo dalla normativa nazionale – il vecchio Codice della privacy (D. Lgs. n. 196/2003) – in quanto prevede maggiore libertà di manovra in capo al titolare. E questa libertà rappresenta l'attuazione del principio dell'*accountability*, infatti il legislatore non impone più le misure minime che il titolare deve adottare nell'effettuare il trattamento dei dati personali, benché promuove la responsabilizzazione di quest'ultimo. Tuttavia questa libertà di manovra concessa al titolare è "un'arma a doppio taglio" perché, se da una parte il titolare non ha vincoli nel predisporre tutte le misure che egli valuta necessarie per garantire la protezione dei dati e quindi adempiere agli obblighi previsti dalla normativa, dall'altra egli è soggetto a sanzioni molto più marcate nel caso in cui risultasse inadempiente.

Per adempiere a questo principio il titolare e, se previsto, il responsabile del trattamento deve adottare misure appropriate ed efficaci per attuare i principi di protezione dei dati, ed essere in grado di dimostrare, qualora richiesto, di aver adottato tali misure. In altre parole, il titolare deve adottare misure tecniche ed organizzative che tengano conto in maniera costante del rischio che un determinato trattamento di dati personali può com-

portare per i diritti e le libertà degli interessati, abbracciando in questo modo un approccio basato sul rischio.

Concernente l'attuazione del principio della responsabilizzazione, il GDPR prevede all'articolo 35 uno strumento utile al titolare finalizzato alla valutazione del rischio inerente al trattamento, la cosiddetta Valutazione d'impatto sulla protezione dei dati (o *Data Protection Impact Assessment – DPIA*). La Valutazione d'impatto è una processo finalizzato a valutare il rispetto dei principi sulla protezione dei dati – in particolare i principi di necessità e proporzionalità rispetto alle finalità del trattamento – e a valutare, nonché a gestire i rischi inerenti al trattamento per i diritti e le libertà fondamentali delle persone fisiche. Dunque il processo di DPIA è il cuore applicativo del principio di Data Protection by design, avente l'obiettivo non solo di garantire la sicurezza dei dati, ma soprattutto di individuare i rischi privacy specifici del trattamento.
Questo processo dovrebbe essere effettuato ogni qualvolta il trattamento presenti un rischio elevato; o sia automatizzato; o tratti, su larga scala, categorie particolari di dati personali di cui all'articolo 9 paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o tratti la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Inoltre si tiene conto delle Linee guida concernenti la DPIA e dei criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del GDPR, adottate dal Gruppo di Lavoro articolo 29. Per quanto concerne il contenuto della DPIA dovrà fornire una descrizione sistematica dei trattamenti, una valutazione della necessità e proporzionalità del trattamento in relazione alle finalità, una valutazione dei rischi, i quali: le modifiche indesiderate dei dati, la violazione o la perdita degli stessi, ed infine la gestione dei rischi, ovvero le misure per mitigare il rischio potenziale.

Inoltre è di fondamentale importanza effettuare la DPIA in via preliminare al trattamento stesso, in quanto solamente una volta conclusa la valutazione d'impatto il titolare del trattamento, sulla base del risultato ottenuto, ovvero il rischio rimanente in seguito all'attuazione delle misure organizzative e tecniche potrà decidere se intraprendere il trattamento o consultarsi con l'Autorità di controllo, come previsto all'articolo 36, GDPR. Quindi l'intervento dell'Autorità sarà principalmente ex post proprio per rafforzare il principio dell'*accountability*, che funge da sfondo all'intero Regolamento.

Sulla base delle indicazioni fornite dalle Linee guida del Gruppo di Lavoro articolo 29 in merito alla DPIA, tenuto conto dell'articolo 35 del GDPR, nonché dei vari principi previsti dalla normativa, si è sviluppato un modello di valutazione di impatto privacy basato sul rischio, composto da quattro sezioni tra loro distinte: la check-list, le informazioni aggiuntive, la sintesi e il masterplan degli interventi.

La prima riguarda determinate situazioni, in merito alle quali verrà calcolato il rischio potenziale, dopo di che verranno effettuate delle attività di controllo con l'intento di capire circa la modalità di gestione delle situazioni stesse. Successivamente si valuterà il presidio, e si calcolerà il "rischio residuo assoluto" e "l'indice di rischio residuo", ovvero il rischio rimanente in seguito alle attività di controllo per ciascuna situazione. Per quanto concerne la seconda sezione, questa funge da completamento alla prima grazie ad una serie di domande finalizzate a fornire ulteriori dettagli circa il trattamento. La terza sezione invece permette di calcolare lo scoring residuo medio, ovvero lo scoring di rischio residuo totale del trattamento. Per arrivare a determinare lo scoring di rischio residuo totale si fa la media aritmetica dei scoring di rischio residuo per ciascuna situazione, e quest'ultimo non è altro che la trasformazione rischio residuo di ciascuna situazione. Infine, l'ultima sezione è dedicata alla fase di monitoraggio e riesame della DPIA, che essendo un processo dinamico, implica una monitoraggio continuo.

Una volta concretizzato il modello di DPIA, questo viene applicato a cinque scenari differenti tra loro, ossia: la videosorveglianza sul luogo di lavoro; i dati medici in azienda ospedaliera; la richiesta del Certificato di Casellario giudiziario a fini assuntivi; telemarketing e l'accesso a banche dati; trattamento dei dati nel settore bancario.

Riguardante il primo scenario, la videosorveglianza sul posto di lavoro, si deve far riferimento oltre alla normativa europea e nazionale, allo Statuto dei Lavoratori – Legge 20 maggio 1970, n. 300, in seguito modificata dal D. Lgs. n. 151/2015 (la cosiddetta Jobs Act) – in particolare l'articolo 4. Tale articolo sancisce che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere utilizzati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Inoltre, l'installazione di queste apparecchiature deve avvenire previo accordo sindacale o, se esso dovesse mancare, previa autorizzazione dell'Ispettorato Nazionale del Lavoro. In assenza del accordo sindacale o dell'autorizzazione dell'INL, il titolare del trattamento rincorre a sanzioni amministrative pecuniarie.

In merito ai dati medici in azienda ospedaliera, questi fanno parte delle categorie particolari di dati, infatti il GDPR gli classifica come dati sensibili. E in quanto tali il loro trattamento è vietato ai sensi dell'articolo 9, paragrafo 1, tuttavia in presenza di determinate circostanze, tale divieto decade. In primis il consenso dell'interessato in virtù dell'attuazione del principio di trasparenza, o nel settore sanitario le circostanze sono riconducibili all'erogazione della prestazione stessa.

Per quanto concerne la richiesta al candidato del Certificato di Casellario giudiziario

da parte del datore di lavoro, questa non può essere fatta, dal momento che il Casellario giudiziario riporta dati relativi a condanne penali e reati, il che implica che il loro trattamento ai sensi dell'articolo 10, GDPR e dell'articolo 2-octies, Codice della Privacy, è permesso solo se, oltre ad essere rispettate le condizioni di liceità previste all'articolo 6, paragrafo 1, vengono soddisfate le seguenti condizioni: il controllo dell'Autorità pubblica e/o l'autorizzazione specifica basata sul diritto dell'UE o dello Stato membro che preveda garanzie appropriate per i diritti e le libertà degli interessati. Dunque il datore di lavoro potrebbe chiedere il certificato di cui sopra solo se autorizzato da una norma di legge, ma dal momento che manca un'autorizzazione legale di questo genere egli non può trattare questa categoria di dati. Se comunque effettuasse la richiesta del Casellario giudiziario, questo implicherebbe l'illiceità del trattamento.

Nel settore del telemarketing vige sia il GDPR sia la legge 11 gennaio 2018, n. 5, recante disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato, entrata in vigore il 4 febbraio 2018. In questo ambito il ruolo fondamentale è giocato dal consenso dell'interessato, in assenza del quale il trattamento risulta illegittimo.

Per quanto riguarda il settore bancario, anche in questo ambito si ha a che fare con un vasto flusso di dati personali, in particolare dati riguardanti la posizione patrimoniale-finanziaria di una persona. In questo caso non sono previsti divieti al trattamento di questa tipologia di dati, tuttavia il titolare deve garantire che il loro trattamento avvenga conformemente al GDPR, il che implica l'attuazione dei principi, l'adempimento alle disposizioni, la tutela dei diritti degli interessati, nonché la valutazione d'impatto sulla protezione dei dati.

L'obbiettivo del presente elaborato è l'applicazione dell'articolo 35 GDPR attraverso l'implementazione di un modello di Valutazione d'impatto sulla protezione dei dati, che potesse essere impiegato in più settori. Tale modello di DPIA costituisce uno strumento importante per la valutazione della responsabilità, in quanto aiuta i titolari non solo a soddisfare i requisiti del GDPR, ma anche a dimostrare che sono state adottate misure idonee a garantire il rispetto del Regolamento.

Capitolo 1

La Privacy e la sua evoluzione storica - giuridica

Il termine "privacy", in italiano viene tradotto con i termini "riservatezza" o "privatezza", viene usato frequentemente nel linguaggio di uso comune così come in ambito filosofico, politico e giuridico, ma non si può affermare il fatto che esista una sua unica definizione, né un suo significato esaustivo. Mentre la parola privacy è rimasta la stessa, non si può dire lo stesso per il suo significato, il quale è in continua evoluzione.

1.1 Il percorso storico del concetto di Privacy

Il concetto di privacy ha antiche e nobili origini, come esposto da Sergio Niger nella sua opera *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*[1]. Niger ripercorre l'evoluzione storica della nozione di privacy, dai tempi dell'Antica Grecia sino ad oggi evidenziando come *"la nozione di privacy non è una nozione unificante. Non è cioè un concetto che esprime esigenze uniformemente e coerentemente diffuse nella storia e nella collettività"*

La nascita del concetto privacy la si identifica ancora nei discorsi filosofici risalenti nell'Antica Grecia. Fin dall'antichità l'uomo ha cercato di proteggersi e di tutelarsi, di appagare il bisogno di trovare dei momenti per essere lasciato in pace per proteggere la propria sfera privata, creando ambienti protetti per lui e i suoi famigliari[2]. Ai tempi di Aristotele si inizia a distinguere tra la sfera privata e quella pubblica: la prima con riferimento alla vita domestica, famigliare e la seconda riferita all'attività politica. Infatti lo stesso Aristotele considerò l'uomo come un "animale sociale-politico"[3], in quanto tale è portato per natura a unirsi ai propri simili per formare delle comunità. È proprio per

[1] S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, Cedam, 2006.

[2] Michele IASELLI e Stefano GORLA, *Storia della Privacy*, Roma, Edizione Lex et Ars, 2015,

[3] Nel trattato "Politica", Aristotele esprime il concetto di "politikòn zôon" (animale politico) che costituisce il riferimento centrale della natura umana.

questo motivo che una persona che dedicava la propria vita solamente alla sfera privata veniva considerata come se non esistesse, condizione degli schiavi a quei tempi. In effetti la partecipazione attiva alla vita pubblica era un obbligo per la parte maschile della società sulla base del presupposto che la partecipazione pubblica fosse la massima espressione dell'eccellenza umana. Chi non intendeva parteciparvi e preferiva prediligere la vita privata era visto con grande disprezzo dagli Ateniesi[4]. Arendt disse: *"Un uomo che vivesse solo una vita privata e che, come lo schiavo, non potesse accedere alla sfera pubblica o che, come il barbaro, avesse scelto di non istituire un tale dominio, non era pienamente umano."*[5]
Infatti, nella cultura greca il poter organizzarsi dal punto di vista politico è totalmente diverso dall'intraprendere quei rapporti naturali che si instaurano all'interno della casa e della famiglia che vi abita avendo al centro l'oikia[6] . Con la nascita della polis, città-stato, come scrive la Arendt: *"Significò per l'uomo ricevere una sorta di seconda vita, il suo bios politikos. Ora ogni cittadino appartiene a due ordini di esistenza; e c'è una netta distinzione nella sua vita tra ciò che è suo proprio (idion) e ciò che è in comune (koinon). Di tutte le attività necessarie e presenti nelle comunità umane, solo due erano stimate politiche e costitutive di quello che Aristotele chiamò il bios politikos, cioè l'azione (praxis) e il discorso (lexis), da cui trae origine il dominio degli affari umani."*[7]

Si vennero a stabilire due modi di esistere: uno naturale – la vita riproduttiva, frutto del bisogno - che si sviluppava nell'ambito della famiglia, separato dalla polis e che restava ai confini della città-stato; l'altro - quello della polis – il linguaggio, era legato ad un modo specifico della politica e aveva a che fare con la libertà. Questa distinzione tra la sfera privata e la sfera pubblica comportava delle conseguenze oltre ai rapporti che vi si instauravano. Infatti nella sfera pubblica vigeva il principio di uguaglianza tra tutti gli uomini, mentre in quella privata vi era disuguaglianza tra i ruoli in quanto nella vita famigliare vigeva il principio del *despotes*, ovvero il ruolo del capofamiglia era alla base della vita famigliare.

Soltanto nel momento in cui il *despotes* partecipava attivamente alla vita pubblica raggiungeva lo stato di libertà: *"[...] quando l'uomo fuoriesce dall'oscura interiorità della casa alla luce della sfera pubblica, [ciò ha] non solo confuso l'antica demarcazione tra il privato e il politico ma ha anche modificato, fino a renderlo irriconoscibile, il significato dei due termini e la loro importanza per la vita dell'individuo e del cittadino."*[8] Quindi la

[4] Arendt esprime così il suo disprezzo:"Una delle caratteristiche della vita privata [...] era che l'uomo esisteva in questa sfera non come un vero essere umano ma solo come un caso della specie animale del genere-umano. Questa, precisamente, fu la ragione ultima dello straordinario disprezzo concepito per essa dall'antichità"

[5] ARENDT H., *Vita activa. La condizione umana*, Milano, Bompiani, 1964.

[6] Oikia dal greco, significa casa; anche la parola economia ha la stessa radice "oikos ", casa

[7] Op. cit. Supra note 5.

[8] Ibidem.

concezione della privacy data dall'autrice, non viene vista come la separazione dalla sfera pubblica, ma viene intesa come luogo di provenienza degli affari collettivi. Infatti la vita famigliare, e quindi la sfera privata è la culla degli affari, in quanto lo spazio domestico è all'origine delle attività economiche.[9]

Così la Arendt:
"Nella sensibilità antica, l'aspetto di deprivazione della privacy, indicato nella parola stessa, era considerato predominante; significava letteralmente uno stato di privazione che poteva toccare facoltà più alte e più umane.[...] Noi non pensiamo più alla privazione quando parliamo di vita privata, e questo è in parte dovuto all'enorme arricchimento della vita privata apportato dall'individualismo moderno. Tuttavia appare anche più importante che la moderna esperienza della privacy è almeno tanto opposta al dominio sociale (sconosciuto agli antichi che ne consideravano il contenuto una faccenda privata), quanto lo è alla sfera politica. Il fatto storico decisivo è che la privacy moderna nella sua funzione più rilevante, quella di proteggere l'intimità, fu scoperta come l'opposto non della sfera politica ma di quella sociale, alla quale è di conseguenza più strettamente e autenticamente connessa"[10]
Un altro filosofo, Platone nella sua opera filosofica, La Repubblica, sosteneva gli stessi ideali, esprimendo la sua volontà per il mescolarsi dell'ambito pubblico con la vita individuale delle persone.[11]

Il concetto di privacy era presente anche nella cultura ellenica. Infatti gli Ateniesi chiamarono le loro case 'recinto/recinzione' (herke), e per questo hanno uno "Zeus Herkeios": essi usavano istallare la statua della divinità nelle loro case affinché proteggesse il recinto delle loro abitazioni e difendesse lo spazio privato dall'esterno. Questa era una modalità con cui si venerava il padre degli dei, Zeus, all'interno dell'ambiente domestico.[12]

Nell'era moderna la sfera politica viene sostituita dalla sfera sociale. Con lo sviluppo del lavoro, delle industrie e della produttività si ha la nascita dell'homo laborans, il quale sostituisce l'ideale di cittadino greco: bravo oratore e coraggioso guerriero.

[9] Op.cit. Supra note 3.
[10] Op. cit. Supra note 5.
[11] "La Repubblica, in greco antico Politéia, è un'opera filosofica in forma di dialogo, scritta approssimativamente tra il 390 e il 360 a.C. dal filosofo greco Platone. In quest'opera tutto ruota intorno al tema della giustizia, sebbene il testo contenga anche una moltitudine di altre teorie platoniche, come il mito allegorico della caverna, la dottrina delle idee, la concezione della filosofia come dialettica, una versione della teoria dell'animadifferente rispetto a quella già trattata nel Fedone e il progetto di una città ideale, governata in base a principi filosofici. Quest'ultima è l'esempio più celebre di quelle teorie politiche che col passare dei secoli prenderanno il nome di utopie. Scritta in forma dialogica, La Repubblica riguarda ciò che viene detto filosofia delle cose umane, e coinvolge argomenti e discipline come l'ontologia, la gnoseologia, la filosofia politica, il collettivismo, il sessismo, l'economia, l'etica medica e l'etica in generale."
[12] Articolo pubblicato sulla pagina web "Lyra - Comunità Hellena italiana", pubblicato da Daphne Varenya Eleusina.

Nell'antica Roma, qualche secolo più tardi, si iniziò a dare maggiore importanza alla sfera privata dei cittadini romani, vietandone l'invasione dei fatti privati in nome della sacralità del focolare domestico.[13]

Col tempo l'uomo ha imparato che oltre alla riservatezza vi sono anche concetti di non minor importanza come la confidenzialità e la segretezza. Ad esempio i messaggi militari insieme a quelli amorosi venivano cifrati.[14]

L'uomo deve ancora ripercorrere molta strada per arrivare a considerare il proprio io e quello degli altri, come ad esempio la considerazione di se stesso, delle sue attività, del suo pensiero, della sua religione, della sua salute, dei suoi affetti, tutte cose che ne determina la propria essenza. Con il Cristianesimo si arriva a definire le caratteristiche più moderne della vita privata dell'individuo, in quanto proprio la moralità cristiana insegnò il rispetto per gli altri, quindi evitando di invadere la dimensione privata altrui ed importunarlo. Ognuno era libero di vivere come meglio credeva, senza sentirsi pregiudicati, perché l'unico giudizio possibile era quello divino.

Proseguendo lungo il sentiero della storia si deve arrivare al medioevo per avere un vero e proprio mutamento della concezione della privacy. Infatti durante il medioevo con l'utilizzo del termine privato si fa riferimento alla vita famigliare dove si veniva ad instaurare un rapporto conviviale basato sulla fiducia reciproca instaurata al interno del focolare domestico. Dunque la privacy costituisce il motivo fondamentale per cui da millenni l'uomo ha costruito dei confini per delimitare la sua proprietà privata: questo bisogno intrinseco della natura umana di demarcare con un linea distinta il confine tra ciò che riguarda la vita privata dell'individuo, in cui si è liberi di agire, pensare ed esprimere i propri sentimenti, pareri senza essere giudicati, ed un sfera pubblica, dove ogni azione, parola e pensiero contribuiscono in qualche modo alla comunità, la quale attribuisce ad ogni atto un certo peso.

Nel medioevo il concetto di Privacy non era ben definito. Infatti tutti sapevano tutto di tutti, perché le persone vivevano in comunità, che si tratti di case, quartieri o villaggi. Di conseguenza la vita era trasparente, e tutte le attività, anche le più intime di un individuo si svolgevano alla luce del sole sotto gli sguardi indiscreti degli abitanti della stessa

[13] Op. Cit. Supra note 5.

[14] Il cifrario di Cesare, con il quale comunicava gli ordini ai suoi generali; il dato non doveva finire nelle mani del nemico. Giulio Cesare "proteggeva" la propria corrispondenza attraverso l'utilizzo di un codice di sostituzione delle lettere del alfabeto, nel quale la lettera chiara veniva sostituita dalla lettera che la segue di tre posti nell'alfabeto (per esempio la lettera C dalla F, e così via, fino a sostituire le ultime tre lettere dell'alfabeto con le prime). Oppure la scacchiera di Polibio, sistema crittografico dal famoso storico greco verso il 150 a.C., che si basava sul frazionamento dei caratteri del messaggio in chiaro così che potessero essere rappresentati utilizzando un più piccolo insieme di simboli.

comunità. Quindi il concetto di privacy del singolo veniva meno, ma anche il concetto di privacy all'interno della famiglia non era tanto rispettato. Infatti come scrivono gli autori M. Iaselli e S. Gorla nella "Storia della Privacy":

"[...] le case erano legate tra loro. Spesso non esistevano porte (ma dei tendaggi), una fila di corridoi univa i vari edifici uno dentro l'altro, con gabinetti in comune nei cortili [...] Le persone dormivano nello stesso letto e condividevano con molti sia i pasti che la casa. Le famiglie erano numerose anche perché venivano integrati nel nucleo individui, parenti, amici, che non riuscivano a provvedere da soli al loro sostentamento (orfani e vedove di guerra, inabili a lavorare per qualche ferita, etc) [...]Non esisteva confine tra tuo e mio, la vita affettiva, lavorativa, l'ozio e il piacere si intrecciavano, il chiacchierare e il parlare si intersecavano coinvolgendo tutti quanti gli appartenenti alla comunità senza scampo. Scomparivano persino i nomi, i cognomi, ognuno veniva indicato dal soprannome, in genere dall'attività o dal mestiere che esercitava. Spesso i nomignoli avevano attinenza con una malformazione o un difetto fisico, noto a tutti."[15]

Nel medioevo il pettegolezzo era all'ordine del giorno inoltre costituiva la causa di gravi problemi. Se per esempio una donna curava le malattie con erbe medicinali poteva essere fatta passare per una strega, di conseguenza finire al rogo.

Durante il feudalesimo il potere pubblico si disgregava in uno *"sbriciolamento che finisce col disseminare i diritti del potere pubblico, di casa in casa, col trasformarsi di ogni grande casa in un piccolo stato sovrano dove si esercita un potere che pur essendo contenuto in una cornice ristretta, pur essendosi infiltrato in seno alla dimora, conserva nondimeno il suo carattere originale che è pubblico"* (Niger, 2006).

Questo per dire che nella società feudale la privacy intesa come sfera privata del singolo era inesistente. Proprio per questo motivo si assiste alla nascita del bisogno dell'intimità individuale, necessità di appartarsi dalle attività in comune, di avere intimità nel campo sociale, religioso, di pensiero. Questo bisogno di intimità viene espresso dal autore Mumford L:*"Il primo mutamento radicale [...] destinato ad infrangere la forma della casa di abitazione medievale fu lo sviluppo del senso di intimità. Questo, infatti, significava la possibilità di appartarsi a volontà dalla vita e dalle occupazioni in comune coi propri associati. Intimità durante il sonno; intimità durante i pasti; intimità nel rituale religioso e sociale; finalmente intimità nel pensiero; [...] ciò segna la fine delle reciproche relazioni sociali fra i ranghi superiori e quelli inferiori del regime feudale: relazioni che avevano mitigato la sua oppressione. Il desiderio di intimità segnò l'inizio di quel nuovo schieramento di classi che era destinato a finire nella lotta di classe senza quartiere e nelle rivendicazioni*

[15]Op. cit. Supra note 2.

individualistiche di un periodo posteriore".[16] Così interpretato da Rodotà:*"questa riflessione di Lewis Mumford coglie il passaggio da un Medioevo dove intimità e solitudine erano appannaggio dei pochi che decidevano di farsi mistici o monaci, pastori o banditi, ad una incipiente modernità nella quale proprio il bisogno di intimità diviene elemento costitutivo del sistema delle relazioni sociali".*[17]

Procedendo lungo il percorso storico si arriva all'inizio del XV secolo,al Rinascimento - epoca segnata di una grande fioritura della vita culturale, colma di manifestazioni artistico-culturale, epoca di rigenerazione dell'umanità.

Nel corso del Rinascimento si assiste oltre al boom culturale, anche ad un grande spostamento demografico dalle campagne alle città. Durante questo processo si osserva una vera e propria esibizione della propria ricchezza, sfoggiando la propria casa. Ecco che la casa ha una funzione ben precisa in questo periodo, quella di mostrare lo status sociale del proprietario. Più la casa era alta ed era costruita con materiale prestigioso più veniva evidenziato il fatto di essere facoltosi. Oltre alla funzione di puro esibizionismo, la dimora costituiva anche il luogo dove si poteva avere della privacy. A quei tempi le famiglie che risiedevano nella città non erano più così numerose come le famiglie rurali, per questo motivo il focolare domestico rappresentava il posto in cui si poteva godere dell'intimità famigliare.

Durante il Rinascimento nell'ambito della politica si afferma il predominio del Signore, ovvero titolo nobiliare che spettava a coloro che detenevano il diritto di svolgere funzioni, amministrare terreni e bene grazie ad una concessione ricevuta da un nobile di rango superiore, che si tratti del re o di un'autorità religiosa con potere di comando e di proprietà. Un'altra figura di rilievo nell'ambito socio-economico è la figura del mercante, la quale con la sua attività commerciale di importatore di beni crea danni economici agli artigiani locali, creando, in questo modo, molte tensioni sociali. Nell'ambito culturale predomina la vita attiva su quella contemplativa, di conseguenza l'artista e lo studioso *"si scostano dalla solitudine della bottega per vivere ed operare in una società dominata dalle regole del bon ton, del gioco, del piacere della tavola e delle relazioni galanti."*[18]

Mentre presso le signorie e le corte dominava il lusso e la bella vita, i poveri dovevano stare molto attenti a tutte le attività intraprese e alle parole dette o anche non dette, per evitare il pericolo di essere puniti anche con condanne molto severe, come torture corporali, morte per impiccagione e persino bruciati sul rogo nel caso si ritenesse si effettuare

[16]MUMFORD L., *La Cultura delle Città*, Milano, Edizioni di Comunità, 1954, p. 29.
[17]RODOTÀ S., *La vita e le regole: tra diritto e non diritto*, Milano, Feltrinelli Editore, 2006, Cit. p. 101.
[18]Op. cit. Supra note 2.

stregonerie. Dunque bisognava stare vigili su ogni fatto e parola, in quanto anche durante il Rinascimento il pettegolezzo continuava ad essere il passatempo preferito di tutti. Ne deriva la grande difficoltà nel fare e nel celare alcuni fatti intimi per l'onnipresenza del pettegolezzo. Quindi la riservatezza della vita famigliare risultava difficile conservare all'esterno. Soltanto all'interno delle corti pare che si era più liberi nell'esprimere la propria parola, perché le corti erano assai modeste.

Si deve ripercorrere ulteriormente la storia fino ad arrivare alla scomparsa della società feudale per avere l'affermazione della privacy nella denotazione di oggigiorno, ovvero una connotazione individualistica. Oltre allo disgregarsi del feudalesimo collaborarono all'evoluzione della connotazione della privacy, secondo Ariès:*"[...]la progressiva costruzione dello stato moderno e lo sviluppo dell'alfabetizzazione."*[19]

Anche dal punto di vista filosofico cambia lo prospettiva di vedere la privacy in modo più moderno. Questo nuovo filone filosofico prese vita grazie ai contributi apportati dal padre del liberalismo classico, John Locke[20] , il quale affermò che i beni privati sono più necessari e urgenti delle cose del mondo comune.[21]

Con il passare degli anni, l'uomo inizia a capire il vero valore dell'intimità, descritta da Arendt come *"un'evasione dal mondo esterno nel suo insieme per rifugiarsi nell'interiore soggettività individuale, che era stata riparata e protetta in precedenza dalla sfera privata"*.[22] Sempre negli stessi anni il filosofo svizzero Jean-Jacques Rousseau incolpa la società della corruzione del cuore umano. Dunque l'intimità non ha ragioni di manifestarsi nella società e tantomeno nel mondo, l'unico suo posto tangibile è la sfera privata.[23] L'individuo dunque ha un bisogno naturale di uno spazio riservato dove poter manifestare la propria intimità e ci dev'essere un armonia tra la sfera pubblica e la sfera privata.

Concludendo l'evoluzione storica della connotazione di privacy, si riportano le parole di Sergio Niger:*"I secoli XVIII e XIX rappresenterebbero secondo autorevoli storici, l'età aurea del privato, in cui si precisano parole e cose e le nozioni si affinano"*.[24].

[19]P. ARIES, *La vita privata*, Laterza, 1988.

[20]John Locke: Filosofo inglese (Wrington, Somersetshire, 1632 - Oates, Essex, 1704). Uno dei promotori dell'Illuminismo inglese ed europeo, fu il primo teorico del regime politico liberale e l'iniziatore dell'indirizzo critico della gnoseologia moderna. (Treccani, 2009)

[21]Il rapporto tra la proprietà privata e la cosa comune viene espresso nel Secondo trattato sul Governo, Cap. V. tratto da "Due trattati sul governo",Plus Edizioni, 1690

[22]Op. cit. Supra note 5.

[23]Ibidem.

[24]Op. cit. Supra note 1

1.2 L'evoluzione giuridica del concetto Privacy

Il concetto Privacy ebbe una connotazione giuridica intesa come diritto di ciascun individuo alla riservatezza con la pubblicazione dell'articolo *"The Right to Privacy"*, apparso il 15 dicembre 1890 sulla Harvard Law Review,[25] da parte di due giovani avvocati di Boston, Samuel D. Warren (1852-1910) e Louis D. Brandeis (1856-1941). I due amici svilupparono un'analisi molto precisa e dettagliata riguardante il rapporto tra il diritto di informare ed essere informati e la riservatezza. Warren e Brandeis erano stati compagni di classe presso la Harvard Law School dove si sono laureati rispettivamente secondo e primo nella loro classe, inoltre tra di loro si era instaurato un rapporto di amicizia da oltre quindici anni. Dopo la laurea presso la Harvard Law School nel 1878, Warren ha iniziato la pratica di diritto a Boston. Un anno dopo ha invitato Brandeis a tornare a Boston da Louisville, Kentucky, per unirsi a lui nella creazione di uno studio legale. Sono stati soci dal 1879 al 1889, quando la morte del padre di Warren, lo costrinse a dimettersi dalla partnership al fine di gestire l'attività del padre.

Brandeis era nato in Germania da una famiglia di ebrei. Fece il liceo classico nella patria, dopo di che venne espatriato insieme alla famiglia negli Stati Uniti d'America. Dopo essersi stabiliti a Louisville nel Kentucky e appena prima dell'entrata di Brandeis nella Harvard Law School, ebbero gravi problemi finanziari. Nonostante le sue origini e i mezzi finanziari ridotti, *"Brandeis fu il più giovane laureato di Harvard, divenne un giudice della Corte Suprema così famoso e così conscio di sé da dire "no" a Roosvelt, dimettendosi quando questi volle piegare la Corte Suprema agli indirizzi del suo New Deal; fece i primi processi a tutela dei minori e dello sfruttamento minorile nello stato di New York, a tutela delle donne, a tutela di cittadini newyorkesi per intercettazioni telefoniche arbitrarie della polizia."*[26]

Warren invece era il figlio di un ricco produttore di carta, e un membro dell'élite commerciale consolidata di Boston. Nel 1883 Warren sposò la figlia del senatore Thomas Francis Bayard, e ciò fortificò ulteriormente la sua posizione all'interno dell'élite di Boston. La moglie di Warren aveva abitudini mondane. Era solita a frequentare club notturni insieme a uomini che non erano il marito. A quell'epoca la stampa era molto interessata al gossip riguardante i personaggi illustri, come lo era l'avvocato Warren, e la loro vita privata. Di conseguenza le abitudini della signora Warren comparivano sulla giornale locale di Boston frequentemente. Questo fatto costituì il movente per cui i due amici - Warren e Brandeis - decisero di scrivere un articolo di impatto scientifico in materia giuridica, intitolato *"The*

[25] BRANDEIS L., WARREN S., *The Right to Privacy*, in Harvard Law Review - Rivista giuridica ritenuta tuttora la più famosa degli Stati Uniti, Volume 4, Articolo 5, 1890. Secondo alcuni autori all'articolo vanno fatte risalire le origini moderne della privacy, mentre giurisdizionalmente la privacy moderna nascerebbe dalle prime sentenze della Corte Suprema degli Stati Uniti.

[26] Informatica libera - blog di Francesco Galgani, articolo del 23 luglio 2014.

Right to privacy", in opposizione agli sconfinamenti della stampa giornalistica grazie alla quale i fatti privati della vita familiare dell'alta società bostoniana, erano quotidianamente alla conoscenza dell'intera comunità. L'articolo scritto dai due avvocati costituisce una riflessione su quali informazioni riguardanti la vita personale di un uomo potevano essere rese pubbliche e quali invece dovevano essere tutelate in quanto dati sensibili, intimi pertanto ritenuti privati.

Dunque gli Stati Uniti rappresentano la culla del diritto alla privacy. Diritto che nasce come mezzo per contrastare gli articoli diffamatori della stampa e si concretizza nel concetto di "right to be let alone"[27] inizialmente riguardante la borghesia. Esso ha subito nel corso degli anni significativi cambiamenti passando da diritto borghese fino ad essere riconosciuto come diritto fondamentale della persona, come tutela della dignità umana. Nella società contemporanea il diritto alla privacy viene inteso come diritto alla protezione, in relazione all'uso e alla circolazione dei propri dati personali, i quali, nella società dell'informazione[28] , ricoprono un fondamentale ruolo. Riguardo a tale affermazione Rodotà scrive:*"Il mutamento di motivazione fa cambiare significato all'invocazione della privacy: nel primo caso, rifiutandosi le informazioni necessarie ai programmi d'intervento sociale, la privacy si presenta come lo strumento per il consolidamento dei privilegi di un gruppo; nell'altro serve a reagire contro l'autoritarismo e contro una politica di discriminazioni basate sulle opinioni politiche. La privacy, in tal modo, diventa un modo per promuovere la parità di trattamento fra i cittadini, per realizzare l'eguaglianza e non per custodire il privilegio, spezzando il suo nesso di identificazione con la classe borghese"*[29].

La privacy assume la cognizione di "diritto" solo in epoca moderna con la trasformazione da espressione di principio a diritto esigibile riconosciuto dalle Carte Costituzionali di tutte le società occidentali e disciplinata da leggi specifiche. Nonostante le specifiche leggi vengano emanate in tempi diversi a seconda dei Paesi, il diritto alla riservatezza viene riconosciuto come diritto fondamentale della persona.

Per la comprensione più chiara del concepimento di una nuova dimensione della privacy con valenza giuridica, quindi come diritto alla privacy, bisogna analizzare il quadro storico sia europeo che del continente oltreoceano, in quanto tale diritto nasce per esigenze diverse a seconda del continente in cui si sviluppa.

[27]GLANCY D. J., riferendosi al "The Right to Privacy" di Warren e Brandeis scrive: *"They placed the right to privacy within the more general category of the individual's right to be let alone"* Glancy, D., 1979. The invention of the right to privacy. Arizona Law Review, 21(1).

[28]Viene denominata società dell'informazione l'attuale società postindustriale caratterizzata dal prevalete di un bene immateriale rappresentato dall'informazione rispetto al bene materiale rappresentato dall'industria.
R. CAFARI PANICO, *Da internet ai social network*, Maggioli Editore, 2013.

[29]RODOTÀ S., *La privacy tra individuo e collettività*, in Politica del diritto, 1974, Cit. p. 551.

Nel continente europeo la privacy assunse la connotazione giuridica già nel lontano fine '700. Il dibattito sull'uso delle garanzie tenuto dal Lord Chatham presso il Parlamento Inglese, nel 1766, è una netta affermazione del diritto alla privacy di ciascun individuo.

"... il più povero degli uomini può, nella sua casetta lanciare una sfida opponendosi a tutte le forze della corona. La casetta può essere fragile, il suo tetto può essere traballante, il vento può soffiare da tutte le parti, la tempesta può entrare e la pioggia può entrare, ma il re d'Inghilterra non può entrare; tutte le sue forze non osano attraversare la soglia di tale casetta in rovina".[30] Il discorso di Lord Chatham funge da tutela del diritto alla privacy anche nei confronti della Corona. Egli attraverso una metafora fa osservare che la privacy, durante l'illuminismo, è concepita come la capacità di una persona nell'opporsi allo "spionaggio" da parte del re. Ma si deve arrivare a metà '800 per assistere all'era aurea della privacy sia nel Vecchio Continente che nel Nuovo. Se da una parte l'uomo inizia ad apprezzare la sfera privata, dove può sentirsi libero di esprimere le proprie idee, i propri pensieri, le proprie emozioni, dall'altra vi è il progresso tecnologico che ha cambiato il vivere quotidiano delle persone invadendo la loro intimità attraverso le nuove scoperte come la stampa e l'editoria.

Una tra le prime legislazioni, che si trova nella storia, avente come fine la tutela della sfera privata degli individui invasa da parte della stampa di continuo è la *Loi relative à la presse* (legge sulla stampa). La legge sulla stampa venne emessa l'11 maggio 1868 in Francia e vietava la pubblicazione di fatti privati degli individui, ad eccezione dei fatti già precedentemente pubblicati con il consenso dell'interessato.[31]

Dunque la tutela del diritto alla privacy – anche se non venivano esplicitamente utilizzati questi termini, in quanto il diritto alla privacy ha origini più recenti – nasce in Francia con la Legge sulla stampa.

Ma si deve aspettare una ventina di anni per assistere all'affermazione del vero e proprio diritto alla privacy nella connotazione contemporanea. Ed è proprio ad opera dei due avvocati bostoniani, entrambi facenti parte della borghesia statunitense, che avviene la nascita del diritto alla riservatezza. In quegli anni la borghesia statunitense raggiunse il suo apice. In effetti in quel contesto la borghesia rappresentava la classe dell'alta società e il diritto alla privacy non era per nulla il diritto naturale di ciascun individuo, ma veniva

[30] William Shakespeare riguardo a Enrico V "Il re prende nota di tutte le loro intenzioni, Con mezzi che nemmeno possono immaginare."

[31] G. G. FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Dordrecht, Springer, 2014.

considerato un diritto esclusivo dell'élite, un privilegio riservato a pochi.

Il contesto storico statunitense del 1890 – anno in cui i due giovani avvocato bostoniani pubblicarono l'articolo *"The Right of Privacy"* – fu caratterizzato da un enorme aumento demografico causato in maggior parte dal fenomeno dell'immigrazione. In effetti, in un secolo – dal 1790 al 1890 – l'Ufficio di Censimento registrò un incremento della popolazione di quasi sessanta milioni di persone.

"Nei decenni tra la fine della guerra civile e il 1890, più di otto milioni di persone erano emigrate negli Stati Uniti. Il continente nordamericano cominciava a riempirsi"[32]. Proprio nel 1890, il Sovrintendente del Censimento dichiarò ufficialmente la chiusura della frontiera. Il fenomeno dell'immigrazione era così intenso che commentatori sociali, come ad esempio Godkin osservarono che *"local life is now much less isolated than it used to be"*, e denunciarono che veniva sempre meno la privacy individuale all'interno delle città sempre più affollate. Questa fu una delle cause che spinsero Warren e Brandeis all'affermazione del concetto giuridico del diritto alla privacy. Ma la causa fondamentale viene individuata nel progresso tecnologico, il quale a quel epoca portò a Boston e nel resto degli Stati Uniti diversi invenzioni che resero la vita degli individui sempre meno riservata grazie all'accessibilità alle informazioni private da parte di altri individui.

Gli Stati Uniti d'America si trovano in uno scenario post bellico, dove era appena finita la Guerra Civile, che aveva diviso e distrutto l'America, ma lo stato Americano riesce a riprendersi in maniera rapida, cambiando la sua struttura politica, economica e sociale balzando verso la modernità. Tale modernità è caratterizzata anche dall'industrializzazione, che muta completamente il panorama americano contadino. Panorama che ha come punto di riferimento la grande città che respira un nuovo clima, quello delle fabbriche, e la nuova classe sociale emergente, quella degli operai. Nei grandi centri urbani, dove le persone sanno solo di lavoro frenetico, si vengono a sfaldare quelle relazioni interpersonali tipiche della campagna, dove la classe contadina legata alla propria terra con la sua quotidianità basata sui rapporti di parentela e di vicinato condividono ogni esperienza ed ogni sapere.

Questo cambiamento – dalla campagna alla città – portò ad una lacuna sul piano sociale, in quanto non si era più all'interno delle piccole comunità dove tutti sapevano tutto di tutti e dove anche i muri avevano occhi e orecchie e dove il *gossip* era considerato il miglior passatempo. Nelle città era impossibile conoscere tutti, mancavano i modelli da seguire, le informazioni utili di cui potersi avvalere e gli eventi di comune interesse da frequentare. Per colmare tale lacuna contribuisce il progresso tecnologico, il quale porta all'invenzione

[32] HANDLIN O., *Out of many: a study guide to cultural pluralism in the United States*, New York: Anti-Defamation League of B'nai B'rith, 1964.

della stampa a rotativa, linotipie[33] ed altri strumenti che permettevano la stampa e la diffusione dei quotidiani in ogni dove. I quotidiani contenevano notizie di ogni interesse, dal più generale al più particolare, senza tralasciare i pettegolezzi locali rendendo sempre più vulnerabili gli individui. Le persone si vedevano pubblicati, parole dette, fatti privati ed immagini che gli riguardavano senza il loro consenso.

Dunque la loro riservatezza veniva violata dalla stampa, la quale ricostruiva la personalità di un individuo rendendola alla portata di tutti. Così le informazioni riguardanti una persona venivano portate al di fuori del cerchio protetto costituito dalla famiglia e dagli amici più ristretti.[34]

1.2.1 La Newspaperization

Alan Westin nel suo libro *Privacy and Freedom*[35], dopo aver fatto un approfondita analisi sul contesto storico in cui prende vita il diritto alla privacy ad opera di Brandeis e Warren, giunge alla conclusione che la classe sociale più colpita dallo sviluppo tecnologico, e quindi presa di mira dai quotidiani, era la borghesia. L'alta società riteneva che le classi sociali inferiori dovessero nutrire il massimo rispetto nei suoi confronti, inoltre non doveva essere recatagli alcuna offesa o danno. Dunque vedere l'esposizione alla pubblica divulgazione dei propri fatti e dei propri vizi, era considerato dall'élite dell'epoca un'ingiustificata offesa che veniva a ledere quel forte sentimento di intangibilità.

Tale fenomeno fu coniato con il termine *"newspaperization"* da Henry James. L'autore individua nella *newspaperization* il punto saliente che fecce prendere la decisione ai due giovani avvocati bostoniani Louis D. Brandeis e Samuel Warren, di preparare una causa contro il giornale, la Evening Gazette di Boston – uno dei primi giornali che faceva uso della stampa a rotativa – il quale pubblicava spesso le abitudini mondane della moglie dello stesso Warren. L'avvocato affermò: *"Questa faccenda dei giornali che si occupano troppo della vita mondana di mia moglie non può continuare"*. Da qui scaturisce la riflessione dei due avvocati su quali informazioni personali di un individuo dovessero essere rese pubbliche e quali, invece, dovessero essere tutelati. Lo scopo del loro articolo e quindi dell'invenzione del diritto alla privacy è stato quello di rivendicare la sensibilità individuale contro la *newspaperization*.

[33] Con il vocabolo "linotipia" si intende il processo di riproduzione fotografica su tela di lino sensibilizzata. Fonte: enciclopedia Treccani.
[34] Op.cit. Supra note 2.
[35] Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1967.

1.2.2 La diffamazione criminale

La violazione del diritto alla riservatezza attraverso la *newspaperization* poteva essere combattuta con un atto legale che a quell'epoca era molto frequente negli Stati Uniti, la diffamazione criminale o la *criminal libel*. Negli anni in cui i due avvocati affermarono il diritto alla privacy,*"accostandolo per analogia alla tutela della reputazione, già riconosciuta dal diritto americano attraverso la previsione della violazione denominata diffamazione"*.[36]. Durante il XIX secolo la legge della diffamazione veniva applicata nei Tribunali statali, quale tutela per la privacy personale. Un caso di diffamazione criminale risalente al 1804 fu quello di "People vs. Crosswell".

Caso People vs. Crosswell

Nel 1804 la Corte Suprema di New York condannò Harry Croswell per aver diffamato il presidente degli Stati Uniti Thomas Jefferson. Crosswell avrebbe infangato la reputazione del Presidente, pubblicando sul giornale di New York, The Evening Post, un articolo intitolato "The Wasp" in cui affermava che T. Jefferson aveva pagato James Callender per fare dichiarazioni sprezzanti su George Washington e John Adams.

Nonostante Crosswell dovesse essere condannato in realtà questo non avvenne, il che porta a connotare la controversia di tale caso rimasto irrisolto. In difesa di Crosswell ricorse l'avvocato Alexander Hamilton che sosteneva l'informazione veritiera. Infatti, dinanzi ai giudici affermò che: *"The right of giving the truth in evidence, in cases of libels, is all-important to the liberties of the people. Truth is an ingredient in the eternal order of things, in judging of the quality of acts"*[37] . E questa posizione di Hamilton sarà poi trasformata in legge dalla legislatura di New York un anno più tardi.

Della stessa opinione dell'avvocato Hamilton fu anche il Cancelliere James Kent, difensore di Crosswell, che vide nella libertà di stampa il diritto di stampare la verità: *"I adopt, in this case, as perfectly correct, the comprehensive and accurate definition of one of the counsel at the bar, that the liberty of the press consists in the right to publish, with impunity, truth, with good motives, and for justifiable ends, whether it respects government, magistracy, or individuals"*.[38]
Dunque la verità veniva utilizzata come difesa contro le accuse di diffamazione, e questo non succedeva soltanto all'interno dello stato di New York ma anche nei vari stati statunitensi. Nel 1890, quando Warren e Brandies scrivono l'articolo sul diritto alla privacy, la pubblicazione della verità non veniva punita secondo la legge della diffamazione. Quindi

[36] F. MODAFFERI, *Lezioni di diritto alla protezione dei dati*, lulu.com, 2015
[37] People v. Croswell, University of Chicago. Retrieved December 13, 2009.
[38] Ibidem.

chi scriveva informazioni vere era tutelato dal diritto alla libertà di espressione, e anche se con la pubblicazione della verità infangava la reputazione di qualche individuo, non doveva scontare alcuna pena per aver infranto la legge della diffamazione. Su questo punto i due avvocati dovettero ragionare per arrivare ad inventare il diritto alla privacy, ritenuto necessario la sua introduzione nel sistema legale statunitense. Questa necessità trova spiegazione nella consapevolezza di Warren e Brandeis del fatto che il rendere pubbliche alcune informazioni riguardanti la vita privata di una persona poteva influenzare e in alcuni casi anche arrecare danni sotto l'aspetto morale e giuridico fino a colpire la parte più intima dell'individuo, riportando le loro stesse parole: la cosiddetta *"his estimate of himself"*.[39] Da qui l'intuizione che il diritto alla privacy nasce da una visione psicologica, campo poco conosciuto a quell'epoca. I due soci interpretarono e definirono nel loro articolo il diritto alla privacy come diritto individuale di proteggere la propria integrità psicologica, come la sua immagine, la sua reputazione, attraverso il controllo sulle informazioni riguardanti la sua personalità. Loro insistettero sul fatto che il diritto alla privacy venisse garantito dai giudici americani nelle loro sentenze affinché questo diritto fosse ben impresso nella mente di tutti i cittadini americani.

In realtà il diritto alla privacy esisteva già nel Common Law e questo lo sapevano bene Brandeis e Warren: *"The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others... fix[ing] the limits of the publicity which shall be given them"*.[40] Infatti loro non utilizzarono l'espressione *"the right to privacy"* ma il diritto di essere lasciati da soli, collocando il diritto alla privacy come un diritto appartenente ad una categoria più ampia del diritto dell'uomo di essere lasciato solo che a sua volta fa parte alla categoria del diritto di godersi la vita, il quale si collocava all'interno della categoria del diritto fondamentale dell'individuo alla vita stessa. Il diritto alla vita fu ed è tuttora uno dei diritti fondamentali, diritti innati individuali riflessi nel V Emendamento della Costituzione degli Stati Uniti d'America emanato dal Congresso il 25 settembre 1789 e rettificato il 15 dicembre 1791:

"No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."

[39] Op. cit. Supra note 25.
[40] Ibidem.

Dunque dire che il diritto alla privacy fu inventato da Samuel Warren e Louis Brandeis non è del tutto esatto. Da quello che i due avvocati stessi dichiararono, emerse che la loro intenzione era quella di inventare una teoria giuridica che facesse chiarezza all'interno del diritto comune, punendo l'attenzione sul diritto alla privacy. A proposito di questo l'autrice Dorothy J. Glancy nel suo articolo citato precedentemente scrisse:

"Warren and Brandeis designed the right to privacy to fill this vacuum by providing legal grounds for individuals victimized by the unconsented publication of true personal information to sue the publishers. Although the right to privacy shared with criminal libel and civil defamation a concern about harm caused by newspaper publicity, Warren and Brandeis did not conceive of the right to privacy as a reincarnation of criminal libel designed to protect the public order from harmful newspaper publicity. Nor did they conceive of the right to privacy as an extension of the civil law of defamation designed to protect the individual's reputation from false publicity. Rather they invented a new concept which would protect a different and otherwise unprotected legal interest: the individual's control over his or her own personality". (Glancy, 1979).[41]

1.2.3 Il confine tra la sfera privata e la sfera pubblica

I due giovani amici partirono dal presupposto che ci fosse qualcosa di privato che deve essere protetto dal fatto di diventare di pubblico dominio. Il diritto alla privacy aveva una funzione ben precisa: quella di tenere la vita privata di un individuo protetta, per evitare che le informazioni private vengano diffuse al pubblico invadente con gravi ripercussioni morali. Questa netta distinzione tra privato e pubblico non riguardava la proprietà, bensì la personalità e i sentimenti più intimi che si possano celare all'interno della personalità di un individuo.

Per arrivare alla distinzione tra pubblico e privato fatta dai due avvocati è necessario fare un passo indietro sul sentiero della storia anglo-americana. Durante il XIX secolo la storia inglese ed americana è connotata dal colonialismo, durante il quale intellettuali, storici e politici vedevano una netta linea di separazione tra la vita pubblica e quella privata: ciò che riguardava la sfera privata aveva come centro d'attenzione il singolo individuo, mentre ciò che riguardava la vita pubblica faceva riferimento alla società, alla comunità.

Nonostante questi concetti fossero fondati nella mente di chiunque, verso la metà del XIX secolo pare che questa netta demarcazione tra pubblico e privato non sia così chiara e distinta in quanto vi mancavano i criteri per effettuare tale delimitazione. E di questo scrisse anche il giurista e il filosofo britannico John Austin in "Lectures on Jurisprudence", lamentandosi di come la giurisprudenza inglese non fosse riuscita a delimitare in modo

[41] Op. cit. Supra note 27.

chiaro e distinto la sfera pubblica dalla sfera privata: *"Every part of the law is in a certain sense public and every part of it is in a certain sense private also... Nothing can be more varying than the views taken by some modern writers of the distinction between public and private law".*[42] Questa critica riguardante la mancante delimitazione tra pubblica e privato riflessa nell'articolo di Warren e Brandeis fu mossa non soltanto dai giuristi dell'epoca ma anche da altri, come dal noto critico James Fenimore Cooper nel suo saggio "The american democrat"[43]:*"there is getting to be so much public right, that private right is overshadowed and lost"* denunciando come:*"another form of oppression practiced by the public, [the public's] arrogating to itself a right to inquire into, and to decide on the private acts of individuals, beyond the cognizance of the laws".* Lo stesso concetto venne affrontato anche dallo scrittore e critico letterario Henry James nei suoi romanzi "The Bostonians"[44] e "The Reverberator"[45], i quali riflettono i rischi, sul piano psicologico e sociale, che si incorrono qualora la vita privata venga sovrapposta dalla vita pubblica. Questo problema fu dibattuto a lungo e costituì il punto centrale del tema privacy affrontato nell'articolo "The Right to privacy".

Dello stesso parere fu anche lo scrittore William Faulkner, vincitore del Premio Nobel nel 1949. Nel 1955, Faulkner visse sulla propria pelle l'invasione della privacy da parte dei giornalisti dopo aver ricevuto ad Oslo l'onorificenza per le sue opere letterarie.

Così Faulkner, preso da una furia memorabile in conseguenza della caccia che i giornali americani stavano dando a fatti della sua vita privata, soprattutto amorosa, scrive un pamphlet micidiale, nel quale prende di mira non solo la stampa americana e la macchina dei media – da lui quotidianamente subita a Hollywood – ma l'intero *Sogno Americano*, venuto meno in quanto nella terra della libertà e della democrazia non si è più capaci di percepire la demarcazione tra ciò che deve essere privato – e come tale custodito e protetto come un tesoro inestimabile – e tra ciò che può essere reso pubblico. Lo scrittore individua nel pubblico, curioso e insaziabile di ficcanasare nella vita privata altrui. In fin dei conti la stampa deve vendere e perciò si adegua a queste richieste di gossip da parte del pubblico. In conclusione pone l'accento sull'importanza della privacy: *"quella privacy che, sola, consente all'artista, allo scienziato e all'umanista di funzionare. O per salvare la vita stessa".*[46] Sulla stessa scia di pensiero fu anche la politologa, filosofa e storica Hannah Arendt che

[42] J. AUSTIN, *Lectures on Jurisprudence*, IV ed. London, Albemarle Street, 1873.

[43] J. F. COOPER, *The american democrat*, I ed., New York, Ed. Barnes e Noble Books 2004, 1838.

[44] "The Bostonians" è un romanzo storico-drammatico scritto da Henry James e pubblicato inizialmente su The Century Magazine, rivista statunitense nel 1885, successivamente avvenne la pubblicazione in volume (in tre tomi) il 16 febbraio 1886 presso Macmillan and Co. di Londra.

[45] "The Reverberator" è un romanzo breve dello scrittore statunitense Henry James, pubblicato nel 1888 originariamente su rivista e subito dopo in volume: la storia è una commedia sociale, sullo stile di Honoré de Balzac, che ripercorre le disavventure che accadono quando storie brute ma vere finiscono per giungere imprevedibilmente nelle pagine dei giornali.

[46] W. FAULKNER, *Privacy. Il sogno americano: che cosa ne è stato?*, Piccola biblioteca Adelphi, 2003.

esprime la necessità *"dell'esser soli con l'idea, l'immagine mentale della cosa da creare"*.[47] Essa vedeva nella privacy, ovvero la garanzia dell'isolamento, una condizione necessaria per poter produrre opere, senza la quale queste ultime non esisterebbero. I motivi che hanno portato a mettere in dubbio il confine tra pubblico e privato sono molteplici. Tra tante cause Warren e Brandeis individuano il progresso tecnologico come una delle cause fondamentali: *"modern enterprise and invention"* e anche la pressione della *"advancing civilization"*.[48] Tra i motivi meno rilevanti si identifica la rinascita di movimenti religiosi che hanno ricongiunto le due sfere – privata e pubblica – *"a grandi ondate di entusiasmo religioso"*.[49]

La soluzione al problema riguardante il confine tra pubblico e privato fu individuata da Warren e Brandeis nella considerazione della forte connessione esistente tra individuo e privato. Arrivarono a definire una specie di autodeterminazione individuale, ovvero dato che la vita privata riguardava ciascun individuo, il singolo individuo doveva decidere quali fatti personali potevano essere resi pubblici e quali invece dovevano restare tra le mura domestiche, protetti e tutelati dalla legge dagli curiosi sguardi indiscreti.

Dunque, la privacy viene riconosciuta come diritto e potere, basandosi su un atto di volontà. La privacy è una legittima pretesa che ciascuna persona ha di decidere con quale modalità e in che misura vuole che le informazioni che lo riguardano vengano rese di pubblico dominio. Di conseguenza il diritto alla privacy venne interpretato come il diritto di ciascun individuo ad avere il controllo sulle informazioni che riguardano lui stesso e la sua vita privata. Stesso concetto viene espresso dallo psicologo sociale Irwin Altman nel suo libro "The environment and social behavior: Privacy, personal space, territory, crowding":

"For my purposes, privacy will be defined as selective control of access to the self or to one's group. [...] Privacy is a central regulatory process by which a person (or group) makes himself more or less accessible and open to others. [...] Privacy is an interpersonal boundary-control process, which paces and regulates interaction with others. Privacy regulation by persons and groups is somewhat like the shifting permeability of a cell membrane. Sometimes the person or group is receptive to outside inputs, and sometimes the person or group closes off contact with the outside environment. [...] Privacy is a dialectic process which involves both a restriction of interaction and a seeking of interaction".[50] Altman scrisse di un personal adjustment process con il quale definisce i confini tra ciò che può

[47] Op. cit. Supra note 5.
[48] Op. cit. Supra note 25.
[49] P. MILLER, *The Life of the Mind in America: From the Revolution to the Civil War*, Harcourt, 1 Ed., 1965.
[50] I. ALTMAN, *The environment and social behavior: Privacy, personal space, territory, crowding*, Montrey, Brooks/Cole Pub. Co., 1975.

essere reso di pubblico dominio e ciò che invece deve essere conservato all'interno del focolare domestico.

L'idea sviluppata da Warren e Brandeis sulla privacy, demarcando il confine tra ciò che è pubblico e ciò che è privato fu ripresa e riaffermata anche da scrittori contemporanei come Robert Ellis Smith in "Ben Franklin's website: Privacy and curiosity from Plymouth Rock to the Internet" e Jeffrey Rosen in "The unwanted gaze: The destruction of privacy in America". Essi scrivono rispettivamente che la privacy è:
"Il desiderio di ognuno di noi di avere uno spazio fisico libero da interruzioni, intrusioni, imbarazzi o responsabilità e il tentativo di controllare il tempo e le modalità di divulgazione di informazioni personali su noi stessi".[51]
"La nostra capacità di controllare sotto quali condizioni rendiamo accessibili le informazione che ci riguardano agli altri".[52]
In questo quadro dove viene teorizzato il diritto alla privacy non bisogna dimenticare il notevole contributo dato dal giurista William Lloyd Prosser con la pubblicazione del articolo "Privacy" avvenuta nel 1960 sulla California Law Review. Il giurista sistematizzò il concetto di privacy e la sua violazione attraverso quattro categorie:

1. Intrusione in uno spazio privato;
2. Rivelare in pubblico i fatti privati personali;
3. Mettere qualcuno in cattiva luce in pubblico;
4. Appropriarsi a fini commerciali del nome o dell'immagine di un privato o di altri suoi dati personali, senza che questi abbia dato il suo consenso.

Grazie al lavoro apportato dal giurista Prosser, le cose iniziarono a cambiare veramente. Infatti, *"a fronte degli 80 casi che tra il 1890 e il 1960 citavano l'articolo di Warren e Brandeis, è stato calcolato che tra il 1960 e il 2007 ce ne sono stati più di 400."*[53]

1.2.4 Diritto alla privacy vs. diritto di essere informati

Dunque la privacy si viene ad affermare come diritto e come tale deve essere tutelato dalla legge. Ma questo diritto – nei casi delle persone illustri che svolgevano cariche pubbliche – andava in contrapposizione con il diritto di essere informati dei normali cittadini. I funzionari pubblici vedevano spesso pubblicate le loro parole, i loro fatti anche senza aver

[51] R. E. SMITH, *Ben Franklin's website: Privacy and curiosity from Plymouth Rock to the Internet*, Privacy Journal, 2000.
[52] J. ROSEN, *The unwanted gaze: The destruction of privacy in America*, New York, Vintage Books, 2001.
[53] M. VALENSISE, pubblica sulla pag. web "il Foglio" l'articolo *The right to be let alone*, in data 19 giugno 2010.

dato l'esplicito consenso. In tal modo la protezione della privacy si poteva considerare quasi inesistente, ma questa inesistenza trova giustificazione nel principio democratico, in quanto i funzionari pubblici dovevano agire nell'interesse legittimo – come tuttora d'altronde – mentre nel caso si tratti di un normale cittadino prevale il diritto alla riservatezza sul diritto di essere informati, in quanto viene meno il principio dell'interesse legittimo.

Nonostante la distinzione teorica tra personaggio pubblico e cittadino normale fosse chiara, non risultava altrettanto chiara la sua applicazione nella pratica. Infatti il confine tra personaggio pubblico e semplice cittadino è demarcato da una linea sottile, in quanto bastava poco per diventare un personaggio pubblico, si pensi ad esempio ad un cittadino normale che ha compiuto un semplice fatto di cronaca. Dal momento che i fatti di cronaca vengono riportati sui quotidiani locali, il semplice cittadino diventa un personaggio pubblico. Ma con il semplice fatto di cronaca si perde il diritto alla riservatezza in quanto prevale il principio dell'interesse legittimo, ovvero l'informazione si ritiene legittima per l'interesse della comunità tale da non garantire più il diritto alla riservatezza o si tratta solo di gossip giornalistico? Da un lato vi è il diritto alla privacy che nel tempo ha acquisito una notevole importanza, tanto da essere considerato diritto fondamentale della persona, e dall'altra parte la libertà di stampa insieme al diritto di essere informati. Warren e Brandeis vedono nel diritto alla privacy come punto di equilibrio tra la riservatezza dell'individuo e l'informazione legittima. I due giovani avvocati inventano il diritto di essere lasciti soli sulla base dell'individualismo, in effetti il punto centrale è rappresentato dall'individuo, il quale nutre il bisogno di essere lasciato in pace e di proteggere le informazioni che riguardano la sua vita, i suoi pensieri, i suoi sentimenti, la sua religione e via dicendo. Tale necessità di essere lasciato solo in isolamento dalla comunità per poter sviluppare la propria personalità – il proprio io – senza essere influenzato dalla società.

1.2.5 L'individualismo moderno alla base del diritto alla privacy

Precedentemente si è accennato il fatto di come il diritto alla privacy nella visione di Brandies ed Warren sia basato sull'individualismo, ovvero *"la tendenza a far prevalere gli interessi o le esigenze personali contro gli interessi o le esigenze della collettività"*,[54] ponendo al centro di ogni studio, analisi e via dicendo, l'individuo.

Le origini dell'individualismo risalgono nel Vecchio continente, con esattezza in Francia ed ebbe una connotazione diversa da quella statunitense. In effetti, con il termine individualismo i francesi descrivevano una situazione a loro sconosciuta e per questo motivo lo individuarono con la parola "egoismo". Infatti Tocqueville scriveva: *"I nostri padri non conoscevano la parola individualismo, che noi abbiamo foggiata per nostro uso. [...] individualismo è un termine recente, originato da un'idea nuova. I nostri padri non cono-*

[54] Definizione fornita dal vocabolario "Treccani".

scevano che l'egoismo".[55] Dunque, originariamente l'individualismo aveva un significato del tutto negativo, il che evidenzia la situazione paradossale tra la cognizione dell'individualismo europeo e quello statunitense. L'individualismo moderno – identificato anche con l'espressione individualismo ideologico – prese vita per mano di alcuni filosofi del XIX secolo, come John Locke e Jean Jacque Rousseau. Questa corrente filosofica, che pone al centro di ogni cosa l'individuo, influenzò le varie costituzioni democratiche. Tant'è vero che l'individualismo ideologico trovò fin da subito inserimento nella costituzione statunitense, che così fu definito da Francesco Lamendola: *"un individualismo virulento, intollerante, tanto astratto quanto velleitario, che pretende di dettar legge alla società, anzi, che concepisce la società in funzione di esso, così che quella diviene semplicemente lo sfondo sul quale l'individuo possa agire, mediante la quale egli possa affermarsi, mentre il compito dello Stato e delle leggi si riduce semplicemente quello di limitare, controllare, imbrigliare la società a favore dei "sacri" diritti individuali"*.[56] Dunque come affermò Lamendola, l'individualismo che si sviluppo durante quei anni era un individualismo spietato che vedeva la società in funzione di esso. L'individuo veniva posto al centro del universo e lo Stato aveva il semplice compito di garantire e verificare che la società non violi i diritti individuali.

Warren e Brandeis sviluppano la nuova concezione del diritto alla privacy sulla base di questa corrente filosofica-ideologica che pone l'individuo al di sopra di tutti e tutto, la prerogativa del singolo domina su quella della comunità. Infatti l'iter del loro articolo si sviluppa ripercorrendo il focus centrale basato sull'individuo. In apertura loro scrivono: *"That the individual shall have full protection in person and in property is a principle as old as the common law"* e continuano su questa linea: *"the common law secures to each individual the right to determining, ordinarily, to what extent his thotiments, and emotions shall be communicated to others"* e concludono il loro saggio considerando sempre l'individuo come punto di riferimento: *"Still, the protection of society must come mainly through a recognition of the rights of the individual"*.[57] Questo continuo riferimento all'individuo come punto centrale dell'intero articolo redatto dai due avvocati rappresenta la riflessione del pensiero liberale[58] sviluppatosi in quell'epoca, il quale vede la profonda radicazione dei

[55] A. DE TOCQUEVILLE, *L'antico regime e la rivoluzione*, a cura di G. Candeloro, Milano, Rizzoli, 1989.

[56] Francesco LAMENDOLA, *L'Individualismo Assoluto della modernità è qualcosa di anti-umano*, in "Arianna Editrice", 29/04/2013

[57] Op. cit. Supra note 25.

[58] Con il Liberalismo si intende: "il movimento di pensiero e di azione politica che riconosce all'individuo un valore autonomo e tende a limitare l'azione statale in base a una costante distinzione di pubblico e di privato. Le premesse del pensiero liberale si trovano nella storia europea a partire dal Rinascimento e dalla Riforma, cioè nella lotta per la libertà religiosa; nella competizione fra la nobiltà inglese e l'assolutismo degli Stuart, che strappò al potere della Corona garanzie sul piano giudiziario e politico; nella dottrina della divisione e dell'equilibrio dei poteri ispirata al modello inglese e teorizzata da C.-L.-S. de Montesquieu; nella concezione di un diritto naturale, fondamento di ogni costruzione giuridica, che da H. van Groot approda al contrattualismo di J.-J. Rousseau.
Altrettanto essenziale è l'individualismo economico dei fisiocratici e della scuola classica inglese, per cui

diritti individuali. Inoltre la teoria neoliberale individua nel diritto alla vita privata un tentativo di valorizzare la posizione dell'individuo nella società borghese, proprio quello che cercarono di fare Warren e Brandeis. Nel loro saggio l'individualismo viene interpretato con una doppia connotazione: sia come un attributo del diritto alla privacy, sia come una protezione per l'individuo.

La prima connotazione riguarda il fatto di vedere nel diritto alla privacy un attributo fondamentale dell'individualismo, in quanto considera i diritti individuali naturali per il fatto che sono innati e quindi ritenuti superiori al sistema giuridico-politico.[59] Infatti la base dell'individualismo di ciascun individuo risiedeva in un diritto fondamentale naturale e il diritto alla privacy veniva concepito come tale. Nel diritto alla privacy si identifica un contributo a ciò che significava essere individuo, in quanto tale diritto rappresenta la facoltà di ciascuna persona di avere il controllo sui fatti privati e poter decidere quali di essi dovevano restare protetti e quali invece, potevano essere di pubblico dominio.

La seconda concezione vede il diritto alla privacy come la funzione di protezione legale dell'individualismo, ideologia di cui si considerava parte integrante, in quanto garantiva una base teorica per assicurare una varietà di rimedi giurisdizionali per punire e/o prevenire interferenze esterne rispetto al controllo di un individuo sulle proprie informazioni personali.[60]
Considerando nell'insieme le due interpretazioni del diritto alla privacy, si può affermare che tale diritto costituisce sia un mezzo che un fine.

Dal punto di vista giuridico, l'applicazione del diritto alla privacy trova giustificazione in quanto attributo naturale dell'essere individuo, ovvero l'autocontrollo individuale sulle

la massima utilità generale è garantita dalla libera competizione, intesa all'utile particolare e svincolata da ogni disciplina (individualismo comune a F. Quesnay, R.-J. Turgot, A. Smith). Le dichiarazioni dei diritti americana (1776) e francese (1789) si pongono al vertice di un processo storico, riassumendone i tratti essenziali: libertà di coscienza e di pensiero, di espressione e di associazione; eguaglianza di fronte alla legge, diritto di concorrere alla formazione della legge stessa, diritto di proprietà.
Il liberalismo ottocentesco si individua nella doppia opposizione contro l'assolutismo dinastico e la democrazia giacobina, nel confronto con l'esperienza storica della Rivoluzione francese e con la realtà della trasformazione industriale. Nel corso del secolo il liberalismo penetra all'interno dei sistemi differenti, dando origine a indirizzi di pensiero in cui la tradizione si incontra con la modernità. [...] Altrettanto evidente risulta, nel liberalismo inglese, la connessione del movimento delle idee con la realtà sociale da cui scaturisce; il liberalismo della scuola di Manchester è espressione della nuova classe in ascesa per l'espansione commerciale e industriale del paese. I principi del liberalismo classico sono ribaditi da J. Stuart Mill: intorno a ciascun individuo c'è una sfera di assoluta libertà, su cui né altri individui, né la collettività possono esercitare un controllo (Principles of political economy, 1848); contro l'arbitrio di una pretesa volontà popolare sono necessarie precauzioni e garanzie, che impediscano la tirannide della maggioranza. Tra le voci discordanti, T.B. Macaulay ammette alcune forme di intervento pubblico e respinge l'atomismo degli utilitaristi; più tardi, L.T. Hobhouse (Liberalism, 1911) ammette alcune forme di tutela delle classi povere." Definizione presa dall'enciclopedia "Treccani".

[59] Per approfondire ulteriormente si veda LOCKE J., The second treatise of government (1st. ed.1690).

[60] Op. cit. Supra note 25.

informazioni riguardanti la propria sfera privata – come i sentimenti, i fatti, le parole, i pensieri e le emozioni – sulla quale si aveva la capacità di controllare in quale misura questa poteva diventare pubblica. Inoltre, il diritto alla privacy poteva essere esercitato in quanto diritto naturale di autodeterminazione dell'individuo, quindi interpretato come mezzo pratico, affermando il potere positivo dell'individuo sul controllo della propria vita, tale che soltanto le informazioni che egli stesso sceglie di condividere con la comunità vengano condivise.[61]

1.2.6 Il diritto alla privacy come estensione del diritto alla proprietà privata

Warren e Brandeis inventarono un nuovo modo di vedere il diritto alla privacy e lo fecero con argomenti ben solidi fondati sulla Common Law. Inoltre fecero una netta distinzione tra il diritto alla privacy e il diritto di proprietà privata. Base del diritto alla riservatezza è costituita dai beni immateriali come i sentimenti, le emozioni i pensieri privati, che rappresentano la sensibilità umana, la quale richiede una protezione della proprietà spirituale dell'uomo. Grazie al loro articolo, i due avvocati bostoniani arrivarono a riconoscere il valore giuridico della sensibilità umana, frutto della continua evoluzione sociale. Infatti i due scrissero: *"ormai si è capito che solo una parte del piacere, del dolore della soddisfazione della vita deriva, per gli uomini, dai beni materiali. Pensieri, emozioni, e sensazioni richiedono dunque, un riconoscimento giuridico, e solo la grande capacità di sviluppo della Common law consente ai giudici di concedere la protezione richiesta, senza l'intervento del corpo legislativo"*.[62]

Punto cruciale emergente dal loro saggio è il paragone tra diritto alla privacy e il diritto alla proprietà intellettuale. Quest'ultimo veniva già tutelato dal sistema giudiziario americano del '800 e riguardava i beni immateriali astratti, come le immagini, i pensieri, i sentimenti le emozioni dell'uomo. Warren e Brandeis individuano il diritto alla riservatezza come una sotto-categoria del diritto alla proprietà individuale. Essi lo classificano come tale in quanto anche il diritto alla privacy intende di svolgere la funzione di proteggere la sfera sentimentale dell'individuo che costituisce la proprietà spirituale dell'uomo. In questo contesto la giurisprudenza veste un ruolo fondamentale, ovvero quello di interpretare al meglio i nuovi bisogni della società in continua evoluzione e garantire una tutela adeguata ai cittadini.

Negli anni della comparsa il saggio, che segnò la nascita del diritto alla privacy, l'uomo non veniva costretto dal sistema statunitense ad esprimere pubblicamente le sue idee, opinioni, emozioni, se non ritenuto necessario per testimoniare nelle aule del tribunale.

[61] Per maggiori approfondimenti si consulti James Q. WHITMAN, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, in "The Yale law journal", Volume 113, N.6, 2004.

[62] Op. cit. Supra note 25.

Ad ogni modo, anche se l'individuo decidesse di esprimere liberamente i propri pensieri, stava a lui decidere in che modo e in quale misura questi potevano essere resi pubblici. L'istituto giuridico che ha la funzione di tutelare i frutti dell'attività intellettuale attraverso il riconoscimento all'autore originario dell'opera di una serie di diritti di carattere sia patrimoniale, che morale viene chiamato il diritto d'autore.[63] Tale diritto ha la finalità protettiva dei beni immateriali come sculture, libri, quadri ed opere musicali, basandosi sulla stessa premessa su cui si fonda la tutela della proprietà privata, ovvero l'aspetto patrimoniale. Ma Warren e Brandeis, individuarono nella tutela del diritto d'autore oltre alla considerazione dell'aspetto economico anche la considerazione dell'aspetto morale – all'epoca non considerato – ovvero l'inviolabilità personale. Per affermare quanto appena detto loro fanno riferimento a tutte le produzioni personali intellettuali, come gli scritti, le opere d'arte che meritano di essere tutelate non contro il furto, bensì contro la loro pubblicazione.

Dunque nel diritto alla privacy si individua una sorta di estensione del diritto alla proprietà privata, in quanto il diritto alla riservatezza riflette la parte emotiva, sentimentale dell'individuo, ovvero la parte del piacere, del dolore, delle soddisfazioni per gli uomini derivante dai beni immateriali. Il principio che i due seguono e hanno in mente nel loro saggio non è tanto il principio della proprietà privata quanto quello dell'inviolabilità personale. Il diritto alla privacy trova una collocazione ben precisa, ovvero nell'ambito della capacità dell'individuo di poter decidere liberamente ciò che della sua vita potrà essere pubblicato e ciò che invece farà parte della sfera privata.

[63] Il vocabolario Treccani definisce il diritto d'autore come segue: "**Il Diritto d'autore** tutela le opere dell'ingegno di carattere creativo riguardanti le scienze, la letteratura, la musica, le arti figurative, l'architettura, il teatro, la cinematografia, la radiodiffusione e, da ultimo, i programmi per elaboratore e le banche dati, qualunque ne sia il modo o la forma di espressione. La tutela autoriale non soggiace ad alcun onere di deposito, come invece si richiede per le invenzioni industriali. Il contenuto del diritto d'autore si articola in diritto morale e diritto patrimoniale d'autore, disciplinati entrambi dalla l. n. 633/1941 e successive modifiche e integrazioni.
Diritto morale d'autore - Il diritto morale d'autore è un diritto personale, inalienabile e intrasmissibile. Si compone di una serie di facoltà, tra cui il diritto di rivendicare la paternità dell'opera e di opporsi a qualsiasi deformazione, mutilazione o altra modificazione dell'opera stessa che possa essere di pregiudizio al suo onore o alla sua reputazione. Tale diritto è inalienabile e dopo la morte dell'autore può essere fatto valere, senza limite di tempo, dal coniuge, dai figli, e, in loro mancanza, dai genitori e dagli ascendenti e dai discendenti diretti; mancando gli ascendenti e i discendenti, dai fratelli e dalle sorelle e dai loro discendenti. Il diritto morale d'autore si concreta anche nella facoltà di non pubblicare l'opera (diritto di inedito), di non rivelare la propria identità al momento della pubblicazione dell'opera e di ritirare l'opera dal commercio, quando ricorrano gravi ragioni morali. Dopo la morte dell'autore, il diritto di pubblicare le opere inedite spetta agli eredi o ai legatari delle opere stesse, salvo che l'autore abbia espressamente vietato la pubblicazione o abbia conferito ad altri tale diritto.
Diritto patrimoniale d'autore - Il diritto patrimoniale d'autore consiste nel diritto esclusivo di sfruttamento economico dell'opera protetta. Si compone di una serie di facoltà, tutte indipendenti tra loro, tra cui la facoltà di riprodurre, distribuire, comunicare al pubblico, tradurre in altra lingua o rielaborare l'opera. Tali facoltà spettano, salvo casi particolari, all'autore o ai suoi aventi causa e hanno una durata limitata nel tempo, potendo lo sfruttamento in esclusiva essere esercitato solo per tutta la vita dell'autore e sino al termine del settantesimo anno solare dopo la sua morte."

In fine, che si tratti della pubblicazione di atti privati da parte di giornalisti accaniti o da pubblicazione di fotografie senza averne il consenso dell'interessato raffigurato veniva fatta una violazione della privacy, diritto tutelato dalla legge statunitense del fine '800 grazie ai contributi apportati da Brandeis e Warren.

1.2.7 Inquadramento giuridico del diritto alla privacy

Per riuscire ad inquadrare il diritto alla privacy in un preciso contesto giuridico statunitense è necessario fare una ricerca nella Costituzione americana.

La Costituzione americana nacque nel 1787 e si basò sulla Magna Carta britannica e sull'originale Dichiarazione dei Diritti risalente al 1776 in Virginia, modificata successivamente nel 1791 nella forma dei Dieci Emendamenti. In realtà, fin dal 1606 – all'epoca in vigore la I Carta della Virginia – in America vigeva la common law della Gran Bretagna con la funzione di garantire *"tutte le libertà, franchigie ed immunità proprie dei liberi cittadini e dei sudditi naturali del Re d'Inghilterra"*.[64] Quindi la prima legislazione americana è connotata dall'esperienza di diritto giurisprudenziale del Europa medievale, ma che in seguito riuscirà a svilupparsi autonomamente.

Inizialmente i Dieci Emendamenti del Bill of Rights venivano applicati ai cittadini americani in quanto cittadini degli Stati Uniti d'America, tralasciando il fatto che spesso accadeva che le leggi dei vari singoli Stati potevano sormontare i diritti previsti dalla Dichiarazione dei Diritti, se diversi da quelli previsti dalla legge locale dei Stati singoli. E queste incomprensione su quale legislazione – locale, di ogni stato, oppure generale, degli Stati Uniti - dovrebbe essere prediletta, continuò fino al 1868, anno in cui venne introdotto il Quattordicesimo Emendamento nella Dichiarazione dei Diritti, il quale vietò chiaramente agli Stati singoli l'approvazione di leggi contrarie al testo originale. In questo modo, ad ogni cittadino statunitense venivano garantiti e resi inviolabili tutti i diritti e le libertà previste dalla Dichiarazione dei Diritti.

Tra tutti i diritti inviolabili previsti sia nel Bill of Rights che nella Costituzione americana,[65] il diritto alla privacy non viene esplicitamente espresso, ma questo non significa che la privacy non sia costituzionalmente tutelata. Storicamente si sono ben due motivi per cui non si è inserito il diritto alla privacy esplicitamente nella Costituzione americana. Il primo risiede nel fatto che il diritto alla privacy era un concetto innato nella società americana, quindi si ritenette inutile esplicitarlo nella Costituzione. Il secondo motivo lo si identifica nel progresso tecnologico, che rappresentò una minaccia per la riservatezza degli individui grazie allo sviluppo dei media, delle telecomunicazioni e all'invenzione dell'editoria e della

[64] M. CASTELLS, *Galassia Internet*, Milano, Feltrinelli,2002.

[65] "[...] la distinzione tra la Costituzione, che disciplina i settori in cui il Governo è autorizzato ad agire, e il Bill of Rights, che nasce per limitare i casi in cui tale azione è possibile." (Iaselli e Gorla, 2015)

stampa.

"Dunque il concetto di privacy, in quanto bene meritevole di protezione, è sempre stato insito nel più vasto campo di quel perseguimento della felicità a cui si riferisce la Dichiarazione d'Indipendenza americana."[66]

Di notevole impatto furono anche le parole pronunciate dall'avvocato Brandeis nella sua dissenting opinion riguardante la causa Olmstead vs. United States del 1928:
"Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions".[67]

ll caso Olmstead vs. il Governo Americano

La causa Olmstead contro il Governo statunitense risale nel 1928, durante il Proibizionismo, che inizio con l'approvazione del Diciottesimo Emendamento, rendendo legge il *National Prohibition Act.* Questa legge vietava la vendita, la distribuzione e il consumo di alcolici.
Roy Olmstead, originario di Seattle, fu condannato con l'accusa di aver contrabbandato alcolici nonostante il *National Prohibition Act.* Ma tale condanna si basava su prove raccolte tramite intercettazioni telefoniche da parte di agenti federali. Queste prove furono ritenute senza valore dagli avvocati di Olmstead, in quanto ottenute senza mandato del giudice in modo illegale perché violavano il Quarto Emendamento che tutelano i cittadini contro "perquisizioni e sequestri ingiustificati" da parte del governo. Ma la controparte, ovvero gli agenti federali, obiettò il fatto che il Quarto Emendamento protegge contro perquisizioni nelle case e sequestri di carte e beni e. Invece loro non erano entrati fisicamente nella casa di Olmstead e non hanno nemmeno preso carte o beni materiali. L'unica azione che fecero gli agenti federali fu quella di intercettare le conversazioni telefoniche che Olmstead ha avuto. Data la complicata situazione di questo caso, in quanto le intercettazioni telefoniche a quell'epoca costituivano una novità, il processo giunse alla Corte Suprema degli Stati Uniti d'America.

La Corte, nel 1928, con la sentenza Olmstead vs. United States, confermò la condanna di Olmstead. Tale decisione fu presa a stretta maggioranza – 5 voti favorevoli contro 4 contrari – tenuta conto anche della *dissenting opinion* del giudice Brandeis. Costui ne

[66] G. SACERDOTI MARIANI, A. REPOSO e M. PATRONO, *Guida alla Costituzione degli Stati Uniti d'America*, Milano, 1999.
[67] L. D. BRANDEIS, *Dissenting opinion in Olmstead vs. U.S.*, 1928.

faceva parte della Corte Suprema degli Stati Uniti d'America dal 1916, anno della sua nomina da parte del presidente Wilson. Nella sua *dissenting opinion* si legge il chiaro collegamento tra il Quarto Emendamento, il Bill of Rights del 1791 e il diritto alla privacy trattato precedentemente nel saggio "The Right to be let alone" insieme all'amico Warren. Infatti egli sostenne che: *"Alla fine del Settecento la forza e la violenza fisica erano gli unici modi che il governo aveva per entrare nella santità della casa e della sfera privata degli individui. E quindi erano state la forza e la violenza fisica a essere regolate dalla Costituzione. Ma i tempi sono cambiati, e mettono a disposizione strumenti più subdoli e potenti di "spionaggio" – che non si fermeranno alle intercettazioni".*[68] Inoltre Brandeis prevede che: *"un giorno potrebbero esserci mezzi con cui il governo, senza rimuovere carte da cassetti segreti, sarà in grado di riprodurle in tribunale e di rivelare a una giuria gli aspetti più intimi della vita domestica".*[69]

In conclusione, il caso di Roy Olmstead iniziò a far riflettere sul Quarto Emendamento messo in relazione con il diritto alla privacy. Dopo soli quattro anni dalla sentenza, Olmstead ottenne dal presidente Roosevelt il *full presidential pardon* insieme al riconoscimento dei suoi diritti costituzionali che sono stati violati da parte degli agenti federali.

Si dovrà attendere il caso Katz vs. United States avvenuto quarant'anni dopo (1967) per veder estesa a tutti gli spazi dove un individuo abbia una "ragionevole aspettativa di privacy" la protezione garantita dal Quarto Emendamento. Alcuni studiosi affermano che questo ribaltamento di logica sia stato influenzato dalla *dissenting opinion* dell'avvocato Brandeis.

1.2.8 Il diritto alla privacy come protezione dell'individuo dalle interferenze governative

Brandeis e Warren vedevano nel diritto alla privacy una doppia protezione dell'individuo, sia da parte degli altri cittadini che da parte del governo americano. Il caso Olmstead costituisce una prova delle interferenze governative nella vita privata di ciascun individuo. Nella sua *dissenting opinion* Brandeis scrisse:

"La protezione garantita [dal Bill of Rights] ha una portata molto più ampia. I padri costituenti intendevano salvaguardare le condizioni favorevoli al perseguimento della felicità. Erano consapevoli del significato della natura spirituale, dei sentimenti e dell'intelletto dell'uomo. Sapevano che le cose materiali sono solo una parte delle pene, dei piaceri e delle soddisfazioni della vita. Degli americani, essi volevano proteggere le convinzioni, i pensieri, le emozioni, le sensazioni. Attribuirono quindi loro, contro il governo, il diritto di essere

[68] Ibidem.
[69] Ibidem.

lasciati in pace [the right to be let alone] – il più onnicomprensivo dei diritti, e quello più apprezzato dagli uomini civilizzati. Per proteggere quel diritto, qualunque intrusione ingiustificata del governo nella privacy dell'individuo, qualunque sia il mezzo impiegato, deve essere considerata una violazione del Quarto emendamento".[70]

In conclusione, Brandeis esprime una considerazione di forte impatto politico:
"E' irrilevante dove sia stata fatta la connessione fisica con i cavi telefonici che portano alle dimore degli imputati. E' anche irrilevante che l'intrusione sia di aiuto alla legge. L'esperienza insegna che dobbiamo stare in guardia e difendere la libertà soprattutto quando gli scopi del governo sono buoni. Gli uomini nati liberi sono per natura attenti a respingere gli attacchi alla libertà da parte di governanti malvagi. I maggiori pericoli per la libertà si annidano invece negli abusi insidiosi di uomini zelanti, in buona fede e mal consigliati. [...] Se il governo diventa un criminale, produce disprezzo per la legge; invita ogni uomo a farsi legge da sé; invita all'anarchia. Dichiarare che, nell'amministrazione della giustizia penale, il fine giustifica i mezzi – dichiarare che il governo può commettere crimini per assicurare la condanna di un criminale – avrebbe conseguenze terribili. Contro questa dottrina perniciosa la Corte dovrebbe schierarsi con risolutezza."[71]

Ma ancor prima della *dissenting opinion*, concetti simili furono espressi nel saggio che Brandeis scrisse insieme all'amico Warren. In "The Right of Privacy" è evidente che il diritto alla privacy funge da protezione dalla interferenze governative:*"The common law has always recognized a man's house as his castle, impregnable, often, even to its own officers engaged in the execution of its commands. Shall the courts thus close the front entrance to constituted authority, and open wide the back door to idle or prurient curiosity?".*[72]

Dunque il Governo deve garantire il diritto alla privacy, ma non deve violarlo. Gli agenti federali sono tenuti al rispetto di tale diritto come tutti gli altri cittadini. Le indagini governative potranno invadere la sfera privata soltanto nel caso sussista un mandato del giudice, oppure nel caso si è avuto l'esplicito consenso da parte della persona interessata. In realtà, la stessa idea fu sviluppata precedentemente anche da altri autori, come il Cancelliere James Kent nella sua opera "Commentaries on American Law" (1826), nella quale identifica nel diritto alla sicurezza personale la protezione dell'individuo, sia da parte del governo e da altri individuali. Un altro esponente della stessa dottrina fu Thomas McIntyre Cooley che nel suo "Treatise on the Law of Torts: Or the Wrongs which Arise Independently of Contract" evidenziò il diritto alla protezione contro le invasioni governative e non della riservatezza di ciascuna persona.

[70] Traduzione a cura di Arnaldo TESTI sul suo blog - "Short cuts America", 18/06/2013.
[71] Ibidem.
[72] Op. cit. Supra note 25.

La questione di porre dei limiti anche al Governo americano nacque con il caso già analizzato in precedenza, ovvero il caso di Olmstead vs. Stati Uniti, che fu il primo caso di intercettazione telefonica nella storia. Questo bisogno di limitare le interferenze governative e non, ma soprattutto quelle governative, nacque per il semplice motivo che nella Costituzione americana non vi era alcuna legge che vietava in modo esplicito le invasioni da parte del governo della privacy. Questa mancanza la si identifica nel fatto che quando si era adottata la Costituzione, non era ritenuto necessario proibire esplicitamente le intrusioni da parte del governo nella vita privata dei cittadini, considerando il principio che il governo non avesse il potere di invadere la riservatezza delle persone. Il porre le limitazioni alle invasioni governative nella sfera privata degli individui iniziò nella seconda metà del XIX secolo, grazie a scrittori e commentatori dell'epoca che avevano a cuore i diritti individuali, tra cui anche il diritto alla privacy previsto nella Dichiarazione dei Diritti. Infatti la maggior parte delle opere di carattere giuridico sviluppava il tema centrato sul diritto individuale alla riservatezza interpretato come limitazione delle invasioni da parte degli agenti federali della libertà personale. Tutti questi trattati si basavano sui diritti espressi nel Terzo, Quarto e Quinto Emendamento. Soprattutto il Quarto, che protegge i cittadini di fronte a perquisizioni e sequestri ingiustificati, mettendo in discussione il diritto alla sicurezza personale e il diritto alla proprietà privata. Dunque il Quarto Emendamento tutela gli individui da ogni intrusione del Governo nelle abitazioni dei cittadini, salvo il caso dell'esistenza di un mandato del tribunale o l'esplicito consenso del proprietario.

Un'esempio né fu il "Treatise on the Constitutional Limitations Which Rest Upon the Legislative Power of the States of the American Union" di Thomas M. Cooley risalente al 1868, in cui tratta la tutela della privacy individuale previsti nel Terzo, Quarto e Quinto Emendamento. Quest'analisi condotta da Cooley venne successivamente applicata dalla Corte Suprema degli Stati Uniti per risolvere il caso Boyd vs. Stati Uniti. Infatti la Corte Suprema durante questa sentenza stabilì che il Quarto ed il Quinto Emendamento della Dichiarazione dei Diritti tutelavano il diritto alla privacy contro tutte le intrusioni del Governo *"nella santità della casa di un uomo e nell'intimità della sua vita"*. Con particolare riguardo all'inviolabilità della casa del cittadino e delle cose private che dovevano restare tali, in quanto diritti innati ed intangibili alla sicurezza personale, alla proprietà privata e alla libertà individuale.

Ma per trovare il diritto alla privacy nella Costituzione americana si deve attendere il 1965, durante la causa Griswold vs. Connecticut. Questo processo si concluse con il riconoscere una tutela federale al diritto alla privacy.

Infine, il Quarto Emendamento è da ritenersi fondamentale per la sua adattabilità al

progresso tecnologico, garantendo ad ogni modo il diritto alla privacy e la limitazione ad ogni forma di controllo da parte del governo.

1.3 Quadro storico europeo: i regimi totalitari

Il quadro storico europeo del XX secolo è caratterizzato principalmente da tre grandi totalitarismi: fascismo, nazismo e stalinismo.[73] I regimi totalitari, pur avendo delle divergenze tra di loro, si fondavano su una stessa ideologia, ovvero quella di alienare l'individuo, privandolo della sua libertà, della facoltà di scelta, di pensiero, e facendogli abbracciare l'ideologia del partito, confortandolo con la propaganda in una rassicurante dittatura, in quanto il totalitarismo si fonda su una continua mobilitazione delle masse.[74] Questo continuo infiltrarsi del politico nell'ambito sociale fu aiutato dall'invenzione e dalla diffusione dei mezzi di comunicazione di massa, grazie ai quali fu possibile arrivare a condizionare ciascuna persona attraverso messaggi insistenti, slogan scritti a caratteri cubitali e discorsi incisivi.

Un altro contributo fu apportato dai mezzi di trasporto, che rendevano possibili spostamenti veloci ed erano in grado di rendere le distanza nulle da consentire controlli in ogni dove. Di notevole importanza fu anche lo sviluppo della psicologia scientifica in grado di apportare tecniche di condizionamento di massa. Il regime totalitario aveva un unico scopo: quello del conseguimento dei valori assoluti come la purezza e il dominio di una razza nel nazionalsocialismo. E per perseguire tale fine dovette reprimere il dissenso ed eliminare ogni spontanea iniziativa, integrando l'intera comunità in un sistema politico chiuso e controllato. In questo sistema il cittadino riceveva una capillare educazione attraverso la propaganda, la quale funge da condizionamento perenne, garantendo così cittadini fedeli

[73] Il termine "totalitarismo" viene così definito dall'enciclopedia Treccani: "Sistema politico autoritario, in cui tutti i poteri sono concentrati in un partito unico, nel suo capo o in un ristretto gruppo dirigente, che tende a dominare l'intera società grazie al controllo centralizzato dell'economia, della politica, della cultura, e alla repressione poliziesca. Storicamente, il concetto di t. nasce con riferimento alle esperienze del fascismo italiano: in un articolo scritto da G. Amendola per Il Mondo, nel 1923, si parla del fascismo come «sistema totalitario» in quanto "promessa del dominio assoluto e dello spadroneggiamento completo e incontrollato nel campo politico e amministrativo" mentre l'uso del sostantivo si fa risalire a L. Basso nel 1925. Fu peraltro lo stesso Mussolini a rivendicare per il fascismo una precisa "volontà totalitaria", capovolgendo il senso dispregiativo del termine. Estendendosi in seguito a connotare sia il regime nazista, sia i vecchi e nuovi sistemi comunisti, il t. è entrato nel linguaggio comune per descrivere una forma politica caratterizzata da assenza di strutture e controlli parlamentari, dalla presenza di un partito unico, dalla soppressione delle garanzie di libertà e pluralismo proprie dello Stato di diritto. Il modello totalitario prevede la preminenza del partito unico sullo Stato; un radicale antipluralismo politico e sociale; l'ideologia della "rivoluzione permanente" e del "nemico oggettivo" per tenere alta la mobilitazione del consenso di massa; l'impiego massiccio delle tecniche di comunicazione come strumenti di propaganda; l'uso sistematico del terrore come strumento di governo. In questo senso i regimi moderni di t. si differenziano non solo dalla democrazia, ma anche dall'autoritarismo, nel quale sono presenti alcuni di questi elementi ma non tutti assieme e con lo stesso grado di intensità. In particolare, i regimi autoritari sono diversi dai regimi totalitari per il fatto di ammettere limitate forme di pluralismo, sia sociale sia politico, nella misura in cui risultino funzionali alle strategie di mantenimento delle riserve di sostegno e di controllo sociale."

[74] H. ARENDT, *Le origini del totalitarismo*, Torino, Piccola biblioteca Einaudi, 1948.

al *dictator*. I dittatori – capi onnipotenti, dotati di carisma – imponevano le ideologie e le regole del regime attraverso la propaganda, la violenza e il terrore, avendo il totale controllo sull'uomo, che doveva solo seguire le regole del regime senza pensare. Il fatto di essere sempre minuziosamente controllati andava a scapito della sfera privata. Dunque il concetto di privacy in un regime totalitario era proprio inesistente, in quanto il regime voleva che ciascun cittadino nutrisse fedeltà totale nei confronti del partito. Il partito ha il pieno controllo sulla vita privata della persone adottando un comportamento non tanto lontano dal *Big Brother* descritto George Orwell nel suo romanzo "1984". Infatti, il partito così come il Grande Fratello sorvegliava giorno e notte i suoi cittadini mirando a conoscere anche gli aspetti più intimi di una persona, con il fine di assicurarsi la massima fedeltà per le sue ideologie e regole. Dunque il potere è onnipresente, è un occhio che gira a 360 gradi, che guarda in ogni angolo della casa e del luogo di lavoro. E questo perenne controllo sembrava che riuscisse a penetrare anche nei pensieri più remoti della persona, violando la propria intimità. Nel regime totalitario nessuno si sente protetto da azioni persecutorie, perché il potere è imprevedibile e il terrore costante. Il regime è in perenne combattimento contro coloro che si oppongono alle sue ideologie e alle sue regole o semplicemente rappresentano potenziale minace per il potere. Tutto questo al fine di legittimare la repressione poliziesca e soprattutto per mantenere quel terrore che giustifichi il continuo cambiamento. E al riguardo di questo, Hannah Arendt, una grande studiosa del fenomeno totalitario, affermò che l'istituzione del "nemico oggettivo" fu una delle proprietà specifiche dei regimi totalitari.[75] Mentre con l'espressione nemico reale viene individuato chiaramente l'oppositore dichiarato e con il nemico potenziale colui che, nonostante non si comporti in maniera ostile, ma per ragioni di appartenenza, o anche frequenza, ad un certo gruppo sociale, potrebbe diventare nemico reale in qualunque momento, il nemico oggettivo si differenzia dagli oppositori diretti e dai potenziali oppositori, perché è l'orientamento politico del governo a determinare la sua identità e non il suo volere di opporsi al potere. Ad ogni modo il regime spesso colpiva a caso senza analizzare se si è di fronte o meno ad un nemico del governo, e faceva questo soprattutto per mantenere il terrore sempre ed ovunque. Durante il dominio del totalitarismo tutto doveva essere letto in chiave politica, e questa nuova ideologia sviluppatasi all'interno della società massificata viene identificata con il fenomeno di iperpoliticizzazione.[76] La caratteristica tipica di questa ideologia di massa è un insieme di comportamenti inattesi, come ad esempio: *"il radicale disinteresse*

[75] Ibidem.

[76] Il vocabolario Treccani riporta il seguente significato: "iperpoliticizzare v. tr. Enfatizzare in maniera eccessiva l'aspetto politico di qualcosa. [Gavino] Angius lo condanna [il governo] per aver posto di fatto una sorta di fiducia, «iperpoliticizzando» un voto che sarebbe stato meglio lasciare del tutto alla libertà di coscienza. È la vecchia tesi cara ai Ds del «passo indietro» che la politica dovrebbe fare sulle questioni etiche, ma l'iter della legge dimostra che a sinistra è mancato per anni piuttosto un passo avanti, sulle questioni etiche e su quelle politicissime – libertà, uguaglianza, laicità – connesse. (Ida Dominijanni, Manifesto, 5 dicembre 2003, p. 4, Politica). Derivato dal v. tr. politicizzare con l'aggiunta del prefisso iper-. Già attestato nella Repubblica del 30 agosto 1984, p. 7 (Enrico Bonerandi).

per la propria persona, la cinica o annoiata indifferenza di fronte alla morte e ad altre catastrofi naturali, l'appassionata tendenza per le idee più astratte come norme di vita, il generale disprezzo per il comune buon senso". (Lamendola, 2013)

Le forze armate del regime totalitario possedevano *"uno sconosciuto spirito di abnegazione".*[77] Questa devozione fu a loro sconosciuta, come spiega Maletta, in quanto non si basava sulla virtù come era solito, ma era mossa *"dal senso della nessuna importanza del proprio io, della propria sacralità. Il militante totalitario è un asceta. La radicale novità dell'ascesi totalitaria rispetto a qualsiasi altra ascesi precedente è che nella prima la lotta contro il male è una questione politica. È questo che costituisce il fattore spiritualmente patologico dell'ideologia. Il male non è più pensato come presente in ogni uomo, ma come incarnato da una classe o da una razza o da un popolo."*[78]

Quindi per epurare la popolazione dal male, il regime totalitario usava metodi disumani, come ad esempio la creazione degli universi concentrazionari, dove venivano rinchiuse, forzate a svolgere duri lavori e infine sterminate milioni di persone. Come ad esempio il campo di concentramento di Dachau, che fu il primo campo di concentramento nazista, quello principale di Auschwitz (Auschwitz I), che insieme al campo di sterminio di Birkenau (Auschwitz II) e il campo di lavoro di Monowitz (Auschwitz III), formavano il complesso concentrazionario situato nelle vicinanze di Auschwitz, in Polonia. Da ricordare anche quello sovietico SLON acronimo di Soloveckij Lager Osobogo Naznačenija (campo per scopi speciali) era un gulag che si trovava sulle Isole Soloveckie, fu ribatezzato con l'espressione Arcipelago Gulag da parte di uno scrittore sovietico dissenziente A.J.Solzenitzyn, il quale denunciò i metodi disumani utilizzati da Stalin durante il suo regime totalitario.

L'universo concentrazionario venne concepito come una struttura politica con la funzione di estirpare dal tessuto sociale quegli individui ritenuti nemici del regime tramite la loro cancellazione della società. Ma l'apice del terrore – il massimo della crudeltà – fu raggiunto nel momento in cui il potere svolse un atto di annientamento della personalità, non tanto attraverso l'omicidio di massa o la deportazione nei campi di concentramento del nemico, quanto la sua completa cancellazione, come se sparisse nel nulla. Così scrisse Sante Maletta nella rivista internazionale di cultura "La Nuova Europa" riguardo il totalitarismo e i campi di concentramento:

"Il sistema dei lager non è un incidente di percorso o un eccesso di crudeltà, bensì è l'esito coerente della mentalità totalitaria: è il modello della nuova società, in cui si realizza la

[77] Sante MALETTA, *Il totalitarismo come forma di pensiero*, in "La Nuova Europa", n. 6, 1999, pp. 78-86.
[78] Ibidem.

scomparsa metafisica dei molti nell'Uno. Il lager non è mezzo ma fine: esso deve azzerare la strutturale capacità di azione umana, la facoltà che ogni essere umano ha di introdurre novità, deve produrre cadaveri, morti o viventi; sentiamo la testimonianza di un testimone diretto: «L'intero sistema del lavoro forzato nella Russia sovietica – in tutti i suoi stadi: interrogatori, udienze, carcere preliminare, e infine il campo – è inteso principalmente non a punire il colpevole, ma piuttosto a sfruttarlo economicamente e trasformarlo psicologicamente [...] Lo scopo reale di un'udienza non è di estorcere al prigioniero la firma a un'accusa fittizia, ma la disintegrazione completa della sua personalità individuale»". (Maletta, 1999)

Dunque l'universo concentrazionario non è un'istituzione penale, creata per la punizione e repressione di delitti e crimini, ma piuttosto una struttura politica di sradicamento del tessuto sociale mediante lo strappo e la cancellazione dalla società di interi settori e gruppi. Infine, il terrore raggiunge il suo apice, la sua punta di raffinata crudeltà, nel lavoro di annientamento della personalità, non tanto uccidendo o deportando il nemico, quanto facendolo sparire. Un recente esempio è costituito dalla Guerra sporca in Argentina. Un programma di repressione violenta con l'intento di porre fine alla cosiddetta sovversione dei gruppi guerriglieri marxisti o peronisti attivi in Argentina dal 1970, e, in generale, abolire qualunque forma di protesta e di dissidenza nel paese presente nell'ambiente culturale, politico, sociale, sindacale e universitario.[79]

Questo programma di repressione raggiunse il suo apice tra il 1976 e il 1979, fu condotta segretamente da parte di unità antisovversive formate dalla polizia federale e dalle forze armate, senza essere controllati. Tali unità mettevano in atto i programmi pianificati e attuati dalla Giunta militare argentina del cosiddetto Processo di riorganizzazione nazionale, capeggiata dal generale Jorge Rafael Videla e dai suoi successori, generali Roberto Eduardo Viola, Leopoldo Galtieri e Reynaldo Bignone. Nell'attuazione di questo programma repressivo vennero violati molti diritti umani e civili della popolazione argentina, in quanto le metodologie di attuazione prevedevano la privazione della libertà senza essere giudicati, la tortura, l'omicidio, la detenzione in posti segreti e le sparizioni delle persone (desaparecidos).

Questo costituisce un esempio storico di come la volontà del capo onnipotente sia superiore anche alle stesse ideologie del regime, che spesso venivano riviste e adeguate in base alle circostanze. Quindi l'unico che possiede il potere assoluto è capo che ha la capacità di decidere su tutto, iniziando dalla risoluzione di qualsiasi conflitto e finendo con la promozione sul piano lavorativo. Nonostante la legge stesse in piedi, questa subisce una completa perdita di valore, in quanto il giudizio finale spetta sempre al *dictator*. Di conseguenza

[79] Guerra Sporca - enciclopedia *Treccani*.

si parla dell'instabilità del regime, in quanto da un lato si proclama di continuo l'ordine sociale, ma dall'altro lato si assiste ad un disordine effettivo sia sul piano legislativo che amministrativo. Un esempio di Stato in cui dominava il caos totale fu considerato il Terzo Reich.[80] Anche se fu mantenuta la Costituzione di Weimar[81] durante il nazismo, questo non impedì al capo ad agire secondo la sua volontà. Perfino l'economia assunse una proprietà dirigista caratterizzante da un continuo intervento dello stato, che imponeva e razionava addirittura i consumi dei suoi cittadini, la cosiddetta "dittatura sui bisogni", che contribuì al potenziamento dell'industria pesante e degli armamenti fino a giungere ad essere autonomi in vista di una guerra.

In questo clima di continua contraddizione e perversione del regime totalitario, l'uomo doveva essere trasparente, che non ha nulla da nascondere. La metafora "l'uomo di vetro" delinea alla perfezione la situazione di ciò che accadeva durante le varie dittature del continente europeo in quegli anni. Sia che si tratti del nazismo sia che si tratti del comunismo, seppur sono stati due fenomeni opposti per le ideologie rispettivamente nell'ambito sociologico, economico e politico, che si seguirono – rispettivamente per il dominio di una razza e per la società senza classi – resta il fatto che il fine di avere il dominio assoluto su tutto e tutti è stato perseguito nei modi più estremi e disumani che esistono, privando l'individuo della propria libertà e della propria privacy. Tutto questo fu compiuto per realizzare la perfezione e l'ordine voluto dal regime a tutti i costi, esigendo da parte dei cittadini la completa sottomissione e condannando chi si opponeva alle regole imposte, perché ritenuto nemico dello stato.

Questo terribile avvenimento dei regimi totalitari insegna all'Europa quanto è di vitale importanza la privacy di una persona. Perché se un individuo viene privato dalla sua propria vita privata insieme alla sua libertà di agire, di pensare e di espressione diventa più una marionetta che un uomo. Tant'è vero che Maletta chiama questo atto con l'espressione "atrofia del giudizio", perché *"Il totalitarismo, insomma, diviene possibilità concreta quando - in una società atomizzata e informata da una mentalità emancipata dalla natura e dalla storia attraverso l'ideologia - il singolo accetta con docilità l'interpretazione dei fatti più propagandata e rifiuta di prendere posizione rispetto a essi"*. (Maletta, 1999)
E il totalitarismo ha la possibilità di affermarsi proprio grazie alla mancanza di volontà e di forza spirituale da parte degli individui.
Dunque la connotazione della privacy diventa in questo contesto totalitario un prerequisito

[80] W. SHIRER, *The Rise and Fall of the Third Reich*, Torino, Einaudi, 1960.
Storia del Terzo Reich(titolo originale "The Rise and Fall of the Third Reich") è un saggio storico del 1960 di William Shirer. Vi si narrano le vicende relative all'ascesa, l'affermazione e la repentina caduta del nazismo in Germania, e della figura umana che ne fu interprete pressoché assoluta, Adolf Hitler.

[81] Costituzione di Weimar dell'11 agosto 1919 fu il primo statuto democratico della storia tedesca e guidò la Germania dalla fine della prima guerra mondiale all'ascesa di Hitler nel 1933.

della democrazia.[82]

"E, proprio in questo caso, i latini avevano pienamente ragione quando affermavano: "Historia magistra vitae". La storia, infatti, deve fungere da momento per ricordarci gli errori del passato, errori che non dobbiamo più commettere. Imparando da essi, possiamo costruire qualcosa di migliore".[83]

Dunque per evitare che un programma repressivo simile si possa attuare nuovamente si deve far riferimento alla memoria. Memoria intesa non soltanto come un accumulo di informazioni, dati, documenti e testimonianze, ma soprattutto come un'approfondita analisi di ciò che è accaduto, l'assunzione di responsabilità e presa di posizione, ovvero ciò che rende l'individuo degno di essere chiamato uomo e cittadino del mondo.

Nonostante il desiderio di non ripetere gli errori del passato sia presente, secondo alcuni studiosi il totalitarismo sia una fenomeno tipico della contemporaneità. Alla base di quanto appena affermata risiedono almeno due motivi di fondamentale importanza. Innanzitutto, la storia contemporanea è caratterizzata dalla società di massa, la quale con i vari fenomeni – segno di modernità – come ad esempio l'alfabetizzazione, l'urbanizzazione e l'industrializzazione, tende a rovinare le tradizionali relazioni tra le persone, indipendentemente dal fatto che si tratti di relazioni di parentela o di vicinato. In effetti, la società moderna, se pur da una parte abbia liberato l'uomo da dittature e schiavitù, dall'altra parte sembra lo abbia isolato. La massa viene vista ed interpretata come un insieme di individui, il quale si qualifica non per il numero, ma per l'assenza di rapporti sociali, fondamentale per l'esistenza degli uomini. Dunque la persona così massificata è vista come una marionetta, che può essere manipolata con maggiore facilità da parte di minoranze organizzative, in quanto è più vulnerabile. Infine il secondo motivo risiede nella continua evoluzione tecnologica, che da un lato apporta importanti invenzioni che facilitano la vita di tutti i giorni, si pensi ad esempio agli *smartphone*, è la rappresentazione di uno strumento multitasking con cui è possibile fare tantissime cose in breve tempo, e dall'altro la perdita delle relazioni intersociali. Oggi giorno si vive una realtà in cui tutti sono amici di tutti sui *social network*, ed estranei sulla strada.

1.4 Dal diritto alla privacy al diritto alla protezione dei dati personali

Il passaggio tra il diritto alla privacy espresso da Warren e Brandeis nel loro saggio *The Right of Privacy* risalente al fine '800 e l'attuale diritto alla protezione dei dati personali

[82] HOSEIN, ROUVROV, POULLET, *Reinventing Data Protection?*, Springer, 2009.

[83] D. MARESCOTTI, *I totalitarismi del XX secolo e la manipolazione delle coscienze*, in "Peacelink", del 20 Marzo 2005.

lo si deve al progresso tecnologico che ribaltò la prospettiva di analisi. All'epoca in cui si sviluppò il diritto alla riservatezza si assistete a nuove invenzioni come la stampa periodica che ha apportato notevoli modifiche nell'ambito sociale, il quale vedeva violata ed invasa la propria sfera privata. Da un lato il progresso tecnologico ha portato la società moderna all'ingresso di una nuova era – quella dell'informazione – segnata da un notevole miglioramento della qualità della vita stessa dell'individuo, dall'altro lato, le nuove tecnologie hanno rivelato anche il loro aspetto negativo, ovvero quello di invadere l'intimità individuale attraverso pubblicazioni di fatti strettamente privati. Quindi da una parte vi era il diritto alla privacy e dall'altra la libertà di stampa e il diritto di essere informati. Si trattava di trovare il giusto bilanciamento tra i vari interessi. Questa armonia non era semplice e facile da raggiungere per la difficile collocazione della nozione di privacy così come si era definita nel sistema legale americano. E proprio per questo motivo negli anni '70 venne proposta l'aggettivazione della parola privacy, rinominata con l'espressione*informational privacy.*

Dunque la prospettiva viene completamente capovolta: mentre prima si cercava di trovare il giusto equilibrio tra la libertà di espressione, il diritto di essere informati e il diritto alla privacy, oggi il focus è quello di proteggere cittadini da *"ogni forma di controllo basato sull'acquisizione di informazioni che possono riguardarli".*[84]

Questa necessità di protezione nasce in risposta alle nuove tecnologie informatiche, le quali vengono impiegate sia da parte della pubbliche amministrazioni che dalle imprese private per perseguire i propri scopi: nel primo caso quello di gestire al meglio la *res* pubblica e nel secondo caso lo scopo lucrativo. Non è un caso che questo fenomeno si verifichi inizialmente negli Stati Uniti d'America, dove l'opinione pubblica della società liberista ha un forte impatto sia sulla pubblica amministrazione – dalla quale pretende una gestione efficiente del bene pubblico, quindi si aspetta una certa trasparenza da parte della PA – sia sull'andamento dell'economia del paese – la quale viene influenzata dai bisogni e dalle preferenze dei cittadini.

Ponendo l'accento sulla trasparenza richiesta alla pubblica amministrazione, il sistema legale statunitense adotto il 4 luglio 1966 dal Presidente Lyndon Johnson il*Freedom of Information Act* (FOIA), ovvero la "Legge sulla libertà di informazione" che ha l'obiettivo di tutelare la libertà d'informazione e il diritto di accesso agli atti amministrativi. Quindi il FOIA stabilisce che chiunque ha diritto di accedere ai registri e agli archivi delle pubbliche amministrazioni. Il Governo ha l'onere di dare spiegazioni nel caso in cui la richiesta di accesso venga rifiutata. Ovviamente l'atto prevede dei casi eccezionali – per esattezza sono

[84] Franco PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, G. Giappichelli Editore, 2016

previste nove eccezioni – per i quali non è possibile consultare alcune informazioni, come ad esempio le informazioni riguardanti la protezione di interessi di ordine superiore come il rispetto della privacy e la sicurezza nazionale.
Il FOIA costituisce un fondamentale strumento di partecipazione attiva del cittadino all'amministrazione pubblica dello Stato, in quanto tale strumento permette a ciascun cittadino di vigilare sull'operato della agenzie federali.[85]

Nonostante gli aspetti positivi di questa legge, ci sono anche quelli negativi, uno di questi è la sua applicazione e la mancanza di una scadenza nel dare informazioni richieste dai cittadini. Per esempio le agenzie federali come CIA, FBI e Pentagono, che possiedono informazioni riguardanti la sicurezza nazionale, quindi di un certo grado di delicatezza, non danno un immediato accesso alle informazioni richieste, nonostante queste non si collochino nei casi di eccezioni previsti dalla legge e di conseguenza rifiutati legittimamente. Per dare una risposta, queste agenzie possono impiegare anche cinque anni, data la mancanza di una disciplina sanzionatoria. E questo lungo termine di risposta fa sì che lo scopo principale del *Freedom of Information Act* non perseguito.
A parte questa problematica, FOIA rappresenta la base normativa in tema di privacy. Su questo primordiale atto poggia il successivo *Privacy Act* del 1974, una legge federale che stabilisce un codice di correttezza e disciplina la raccolta, l'uso e la diffusione di informazioni riguardanti i cittadini mantenute nei sistemi di registrazione presso le agenzie federali. Il *Privacy Act* nasce per porre fine agli abusi apportati ai cittadini da parte delle pubbliche amministrazioni e delle agenzie federali, le quali facevano un uso improprio delle informazioni a disposizione. Fu lo scandalo Watergate[86] – nel quale era stato coinvolto lo stesso presidente Nixon, che finì per dimettersi a seguito di tale scandalo – a far presente l'assoluto bisogno di una legge che regolasse e limitasse l'operato delle agenzie federali e degli enti pubblici in tema di privacy.

Al primo impatto sembra che FOIA e *Privacy Act* andassero in direzioni opposte: mentre la legge sulla libertà di informazione consente a chiunque di accedere ai dati dei privati che sono mantenuti presso gli enti pubblici, la legge sulla privacy invece ha lo scopo di

[85] Dipartimento di Giustizia degli Stati Unini d'America, *What is FOIA?*

[86] Così Iaselli e Gorla nel libro "La Storia della Privacy": *"Ma fu un evento, in particolare, a far scattare l'esigenza di una legge che tutelasse gli individui da interferenze non giustificate. Il 17 giugno 1972 vengono arrestati cinque uomini, nel tentativo di inserire delle cimici nei telefoni degli uffici del Comitato Nazionale del partito democratico, con sede presso l'hotel Watergate. Grazie anche all'inchiesta di due giornalisti del noto quotidiano Washington Post, due dei cinque uomini arrestati vengono ben presto identificati come ex agenti della CIA, molto vicini al presidente repubblicano Nixon. Nonostante i primi tentativi di insabbiamento, lo scandalo che ne segue è di proporzioni enormi. Tutti i cittadini americani, sempre più allarmati, seguono in diretta gli atti di un processo che porterà alle dimissioni del presidente, e durante il quale le potenzialità delle intercettazioni telefoniche e delle cimici spia sono ben sviscerate, sotto gli occhi di tutti. Una legge sulla privacy, che ponesse un freno agli svariati abusi commessi nell'uso delle informazioni che le agenzie e gli enti pubblici avevano a disposizione a riguardo dei cittadini, si rendeva assolutamente necessaria."*(Iaselli e Gorla, 2015)

proteggere, mantenendo confidenziali tali dati. In realtà gli obiettivi di entrambe le leggi non sono poi tanto così diversi. Infatti entrambi gli atti hanno l'intento di trovare il giusto equilibrio tra il diritto dei cittadini di essere informati sull'operato del governo e degli enti pubblici e il diritto individuale a salvaguardare la propria privacy.

Seppur siano stati passati tanti anni dal *Privacy Act*, questo rimane uno tra gli atti principali aventi lo scopo di proteggere la privacy dei cittadini americani. Uno dei punti dolenti della legge sulla privacy è il suo campo di applicazione, dal quale rimangono esclusi i rapporti tra i soggetti privati, dato che questa norma regola esclusivamente i rapporti tra cittadino ed enti pubblici o/e agenzie federali. Inoltre, dal punto di vista territoriale, il *Privacy Act* regola solo trattamenti di dati dei cittadini americani.

Successivamente sono state emanate altre leggi in tema di privacy seppur sempre applicabili in ambiti particolari, come ad esempio la *Tax Reform Act* del 1976 che ebbe lo scopo di proteggere la privacy riguardante dati di natura finanziari. Un altro atto che tutelava la privacy dei guidatori rissale al 1994, il cosiddetto *Driver's Privacy Protection Act*, questa normativa impediva il rilascio di informazioni personali riguardanti un determinato guidatore senza il suo esplicito consenso.
Dunque si può venire alla conclusione che negli Stati Uniti il tema della privacy viene affrontata settorialmente con leggi emanate ad hoc. In questo sistema settoriale della privacy in cui al cittadino viene associato lo status del consumatore,[87] di conseguenza la tutela della privacy viene garantita sostanzialmente attraverso due regolamentazioni. La prima regolamentazione segue i principi del *fair information practice*, basatasi principalmente sull'informativa per il consumatore, una richiesta di consenso, la possibilità di accedere e verificare i dati, garanzie di conservazione in sicurezza dei dati e misure atte a rispettare tali principi. La seconda regolamentazione si fonda sul sistema *permissible purpose*, la quale pone dei limiti al trattamento dei dati a finalità previste dalle leggi.[88] Questa lacuna di generalità della legge federale e la sua applicazione settoriale per quanto riguarda la tutela della privacy viene evidenziata anche da parte dell'autrice Lucia Miglietti sulla rivista Diritti Comparati, infatti essa scrive: *"Le leggi degli Stati Uniti perseguono l'obiettivo di regolamentare il trattamento dei dati in ambiti specifici di attività economica, nella misura in cui vi possano essere rischi per il cittadino considerato nel suo status di consumatore. Ne consegue che negli USA, differentemente dall'Europa, la privacy non si configura come un diritto fondamentale dell'individuo, ma come un diritto del consumatore, da bilanciare con le esigenze delle imprese."*[89]

[87] L'autorità vigilante sul rispetto delle leggi da parte delle imprese è il Federal Trade Commission.
[88] P. SWIRE, S. BERMANN, *Information privacy*, IAPP Publication, 2007.
[89] L. MIGLIETTI, *Profili storico-comparativi del diritto alla privacy*, sulla rivista Diritti Comparati, 2014.

Nonostante la privacy venga tutelata per settori senza una normativa generale che possa essere valida ed applicabile in tutti i settori e per tutti i cittadini, non soltanto per i cittadini americani. Il diritto alla privacy venne ulteriormente limitato con l'approvazione da parte del Senato americano dell'*USA Patriot Act* , acronimo di *Uniting and Strengthening America by Providing Appropriate Tool Required to Intercept and Obstruct Terrorism Act* del 25 Ottobre 2001, convertito in legge dalla firma del presidente George W. Bush il giorno successivo. L'*USA Patriot Act* venne emanato in seguito agli attentati terroristici del 11 Settembre 2001, "Martedì delle Tenebre" il giorno che segnò tragicamente non soltanto la grande potenza statunitense ma l'intero mondo.
I colpevoli di questo tragico evento sono stati individuati con le più grandi agenzie federali, l'FBI e la CIA, in quanto non hanno intercettato nessun segnale per poter prevedere l'attacco terroristico, nonostante i potentissimi mezzi a disposizione.

Così Iaselli e Gorla scrivono: *"Le polemiche colpirono anche il famigerato Echelon, il Grande Orecchio elettronico puntato dai servizi segreti americani sul resto del mondo, rivelatosi completamente sordo nel momento più critico degli Stati Uniti dalla fine dell'ultima guerra mondiale. Ma tralasciando le inevitabili recriminazioni che hanno seguito l'attentato al World Trade Center, quello che importa rilevare è che le uniche vittime dell'11 Settembre 2001 non furono i morti causati dai dirottamenti aerei e dalla guerra che ne è seguita. La tragedia delle Torri Gemelle ha accelerato drammaticamente un processo già in corso negli Stati Uniti da molti anni: le libertà individuali garantite dal Bill of Rights del 1791 hanno cominciato a divenire un bersaglio sempre più fragile della guerra al terrorismo proclamata dal Presidente Bush all'indomani della strage."*[90]

In sostanza l'*USA Patriot Act*, è un insieme di provvedimenti che rafforzavano i poteri della polizia in ogni ambito, specialmente nell'ambito del controllo sulle comunicazioni.

"O, più esattamente, volendo ripetere le parole pronunciate dal presidente George W. Bush nel firmare la legge, una sommatoria di provvedimenti tesi a "porre i sistemi di sicurezza nazionale all'altezza della sfida generata dalla proliferazione delle tecnologie di comunicazione, leggi nate nell'epoca dei rotary telephones". Sul piano tecnologico, poi, l'amministrazione americana è stata rapidissima nel presentare un progetto molto dettagliato e già completo, denominato Total Information Awareness (TIA), ma subito ribattezzato dall'Electronic Privacy Information Center (EPIC) "Terrorism Information Awareness", e per fortuna rimasto solo un progetto." (Iaselli e Gorla, 2015)

Dunque l'*USA Patriot Act* è una norma che ha come fine quello di garantire la sicurezza nazionale, tramite il consenso alle agenzie federali all'accesso a strumenti utili, come le in-

[90] Op. cit. Supra note 2.

tercettazioni telefoniche, la lettura delle mail private, per riuscire ad anticipare gli attacchi terroristici. Se da una parte il *Patriot Act* garantisce la sicurezza nazionale, dall'altra viola dei diritti fondamentali dei cittadini statunitensi, in primis il diritto alla privacy. Bellazzi al riguardo scrive:

"Essa aumenta la possibilità per gli organi di polizia di intercettare le comunicazioni via telefono o computer, di eseguire perquisizioni all'interno di abitazioni o uffici all'insaputa del proprietario, di prelevare da biblioteche, istituti di credito, ospedali, scuole documenti riguardanti aspetti strettamente personali di qualsiasi individuo, dalle sue condizioni di salute, alla sua situazione economica, ai libri che legge, e consente al Governo di detenere, in presenza di particolari condizioni, senza limiti di tempo, lo straniero che abbia violato le leggi sull'immigrazione o sia ritenuto una minaccia per la sicurezza nazionale".[91]

Questo ampliamento dei poteri delle agenzie dell'*intelligence* e delle forze dell'ordine permettendo loro l'accesso ad informazioni personali, violando così il diritto alla privacy.

In conclusione, si può affermare che il sistema giudiziario statunitense è più incline alla protezione della sicurezza nazionale che alla protezione dei dati personali, ponendo gli interessi della collettività al di sopra degli interessi del singolo. Se invece si fa riferimento alla normativa del continente europeo, la prospettiva è completamente rovesciata. Con riguardo a quanto appena affermato si riportano le parole espresse da Edoardo Alberto Rossi sulla rivista di diritto pubblico italiano, comparato, europeo "Federalismi.it": *"[la normativa europea è] caratterizzata da un maggiore garantismo in tema di privacy e protezione dati".*

Dunque per analizzare l'evoluzione giuridica del concetto di privacy nella connotazione più vicina a quest'epoca bisogna spostarsi nel continente europeo.

[91] M. BELLAZZI, *I "Patriot Acts" e la limitazione dei diritti costituzionali negli Stati Uniti*, nella rivista "Politica del Diritto", Il Mulino, XXXIV, n.4, 2003, pp. 681-706.

Capitolo 2

La legislazione europea in materia di Privacy antecedente al nuovo "Pacchetto Protezione Dati"

Il continente europeo si può considerare il principale fondatore del diritto alla privacy, in quanto rappresenta il luogo per eccellenza dove nasce il diritto alla privacy e la protezione dei dati personali. La connotazione europea della privacy è ben diversa dalla connotazione statunitense. La spiegazione risiede nella storia del continente europeo della prima metà del '900, epoca dei regimi totalitari, i quali hanno segnato profondamente la vita di moltissime persone. Nel momento in cui si arrivò al tramonto delle varie dittature, che si instaurarono nel continente europeo, la privacy iniziò ad assumere un valore di vitale importanza nella mentalità delle persone.

In seguito al terrore instaurato dai vari regimi totalitari, all'interno della società nacque il bisogno di avere una protezione dell'individuo, delle sue libertà con lo scopo di evitare il terribile episodio accaduto durante quegli anni. Dunque vi è necessaria una legislazione europea in materia di privacy. Esistono numerose fonti normative riguardanti il diritto alla privacy, e queste devono essere lette in chiave generale per riuscire a caratterizzare il diritto alla privacy.

Francesco Maria Pizzetti scrive riguardo al diritto alla privacy: *"il diritto europeo in materia di protezione dei dati come un complesso sistema di regole e principi che incrociano tra loro atti normativi appartenenti a due diversi ordinamenti: il Consiglio di Europa e l'Unione europea. Ciascuno dei due ordinamenti ha un proprio sistema di fonti e allo stesso modo un proprio sistema di Corti, che, nonostante siano spesso intrecciati negli effetti che determinano, devono essere tenuti separati dal punto di vista concettuale."*[1]

[1] F. M. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali*, Torino, G. Giappichelli Editore, 2016.

2.1 Il Consiglio d'Europa e la CEDU

All'indomani della Seconda Guerra Mondiale viene costituito con il Trattato di Londra il 5 maggio 1949 il Consiglio d'Europa con sede a Strasburgo, in Francia, nel Palazzo d'Europa e ha due lingue ufficiali: l'Inglese e il Francese. Alla sua costituzione aderirono 10 Stati[2] e successivamente aderirono anche altri fino ad arrivare a contare oggi 47 Paesi, di cui 28 fanno parte dell'Unione Europea. Il Consiglio d'Europa venne costituito con l'intento *"di riunire gli Stati d'Europa e promuovere lo Stato di diritto, la democrazia, i diritti dell'uomo e lo sviluppo sociale. A tal fine, nel 1950 esso ha adottato la CEDU,*[3] *entrata in vigore nel 1953."*[4]

Dunque nel 1950 all'interno del Consiglio d'Europa venne adottata la Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali, individuata con l'acronimo CEDU, entrata in vigore nel 1953.[5] Tutti gli Stati che vi hanno aderito hanno l'obbligo internazionale di attenersi a quanto stabilito nella CEDU, rendendo le leggi nazionali conformi ad essa.

"La CEDU rappresenta il primo trattato che mira alla tutela dell'individuo e ancora oggi l'unico dotato di un meccanismo giurisdizionale permanente di garanzia, al quale ogni persona può richiedere la salvaguardia dei diritti garantiti dalla Convenzione".[6]

Quindi la CEDU viene considerata il più importante strumento giuridico in materia di diritti umani e libertà a livello europeo, tra cui anche il diritto al rispetto della vita privata e familiare espresso nell'articolo 8 della Convenzione. L'articolo 8 stabilisce che:

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

2. *Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una*

[2] I paesi che diedero vita inizialmente al Consiglio d'Europa sono: Belgio, Danimarca, Francia, Irlanda, Italia, Lussemburgo, Norvegia, Paesi Bassi, Regno Unito e Svezia. Tra il 1949 e il 1950 si aggiungono poi Germania, Grecia, Islanda e Turchia. Nel 1956 l'Austria, nel 1961 Cipro, nel 1963 la Svizzera, nel 1965 Malta.

[3] In Inglese: "Convention for the Protection of Human Rights and Fundamental Freedoms", o ECHR

[4] Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018.

[5] "La Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali è stata firmata a Roma il 4 Novembre 1950 ed è entrata in vigore il 3 settembre 1953 in seguito al deposito di almeno dieci strumenti di ratifica. Per l'Italia l'entrata in vigore avvenne solo il 10 ottobre 1955; dopo una lunga elaborazione giurisprudenziale, è però dopo le cosiddette sentenze gemelle (n. 348 e 349 del 2007) della Corte costituzionale che la cogenza nella Convenzione in Italia si è assai rafforzata, restando esclusa la possibilità «di attribuire agli enunciati convenzionali significati diversi e incompatibili con quelli assegnatigli dalla Corte di Strasburgo. Sono oggi parte del trattato tutti e 47 i paesi membri del Consiglio d'Europa."

[6] P. GIANNITI, *La CEDU e il ruolo delle corti*, Bologna, Zanichelli, 2015.

società democratica, è necessaria per la sicurezza nazionale, per la pubblica sicurezza, per il benessere economico del paese, per la difesa dell'ordine e per la prevenzione dei reati, per la protezione della salute o della morale, o per la protezione dei diritti e delle libertà altrui."

Dunque il primo comma dell'artt. 8 stabilisce che ogni persona ha diritto al rispetto della sua vita privata e famigliare, mentre il secondo comma elenca i casi in cui un'autorità pubblica può mettere a restrizioni tale diritto, si tratta di casi eccezionali quali l'ordine pubblico e la sicurezza nazionale.
L'articolo 8 della CEDU verrà considerato come una normativa che tutela il diritto alla privacy.

Per garantire che gli Stati membri adempiano ai propri obblighi stabiliti dalla Convenzione, nel 1959 è stata istituita la Corte EDU a Strasburgo. La Corte EDU garantisce che gli Stati adempiano gli obblighi previsti dalla Convenzione valutando le denunce riguardanti l'esistenza di violazioni della CEDU presentate da persone fisiche o persone giuridiche. La Corte EDU ha inoltre la facoltà di esaminare le cause interstatali intentate da uno o più Stati membri del Consiglio d'Europa contro un altro Stato membro.[7]

In qualità di organo giurisdizionale internazionale, la Corte Europea dei Diritti Umani copre la funzione consultiva e contenziosa. Con funzione consultiva interviene su richiesta del Comitato dei Ministri riguardo l'interpretazione della CEDU e dei relativi protocolli addizionali. Mentre la funzione contenziosa è dovuta al fatto che ha la facoltà di decidere in merito ai ricorsi sia degli Stati membri, sia dei singoli individui – non necessariamente cittadini di uno degli Stati membri – che denunciano una violazione di un diritto stabilito dalla CEDU. Quest'ultimo può esser fatto in seguito ad una prova di aver fatto ricorso giurisdizionale nazionale ordinario senza esito o con esito non soddisfacente. Per questo motivo si può dire che la Corte EDU rispetto alla giurisdizione nazionale ha funzione sussidiaria. Infatti essa, in seguito al giudizio espresso dai giudici nazionali, verifica se tale giudizio sia o meno compatibile con la normativa stabilita dalla Convenzione.

2.1.1 Le sentenze della Corte EDU

La Corte EDU ha risolto molti casi in merito alla materia di protezione dei dati personali, in particolare, in moltissime cause ha apportato la sua interpretazione dell'articolo 8 della CEDU, il quale tutela la vita privata di ciascun individuo. Tale articolo, in seguito alle varie sentenze della Corte Europea sui Diritti dell'uomo, è stato definito in modo più chiaro. Lo stesso concetto di dati personali riguarda un ambito più vasto che oltre a com-

[7] Op. cit. Supra note 4.

prendere le generalità, include al suo interno anche il DNA e le impronte digitali.

Un esempio né è il caso *S. e Marper vs. il Regno Unito.*
S. e Marper – due cittadini inglesi – sono stati accusati in passato, rispettivamente di rapina e violenza sessuale. In quella sede furono raccolte le rispettive impronte digitali e campioni di DNA, in quanto la legge inglese prevedeva il prelievo coattivo di materiale biologico appartenenti a individui condannati, indagati o sospettati. La legislazione inglese prevedeva la conservazione di tali campioni a tempo indeterminato anche nei casi in cui gli individui venivano scagionati da ogni colpa, in quanto innocenti. Una volta dimostrata la loro innocenza, S. e Marper richiesero la distruzione dei loro dati personali dal database nazionale. Ma la loro richiesta fu respinta, perché appunto la legge non prevedeva un termine prestabilito per la conservazione dei dati. Quindi i due hanno agito nei confronti dello Stato inglese, ritenuto l'unico responsabile del funzionamento del database nazionale e dell'operato delle forze dell'ordine, inizialmente dinanzi alle Corti nazionali, e successivamente hanno fatto ricorso alla Corte EDU.

La Corte di Strasburgo nella sentenza del 4 dicembre 2008 in merito a tale caso espresse la violazione dell'articolo 8 della Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali da parte dello Stato inglese. Infatti la Corte affermò il fatto che dai campioni biologici si potevano ricavare dati sensibili riguardanti una persona, come ad esempio il suo stato di salute. Quindi la conservazione di tali informazioni sensibili costituiva un'invasione della vita privata dell'individuo. Si osservò inoltre che dal DNA era possibile ottenere informazioni unici riconducibili a relazioni genetiche tra gli individui, compromettendo in certi casi la propria vita privata. Oltre alle informazioni genetiche, dal DNA si possono derivare informazioni circa le origini etniche di una persona, rendendo ancor più vulnerabile l'individuo.

Per quel che riguarda le impronte digitali, queste contengono minor numero di informazioni rispetto al DNA, ma non per questo la conservazione di esse è da ritenersi di minor ingerenza nella sfera privata.

Dunque la Corte di Strasburgo giunse alla conclusione che la pura conservazione di dati genetici costituisce un'intrusione nella vita privata dell'individuo e quindi una violazione dell'articolo 8 della CEDU, il quale tutela il diritto al rispetto della vita privata di ciascuna persona. Una simile interferenza da parte delle autorità nella sfera privata è ammissibile se rispetta alcuni principi di vitale importanza per una società basata sulla democrazia, quali il principio di legalità, di finalità ed infine di necessità. Dunque la conservazione dei dati personali è possibile se la legge lo ammette. Il rispetto di tale principio costituisce un requisito formale. Inoltre è richiesta che sia esplicita la finalità per cui vengono trattenuti

i dati personali. Nella finalità si individua un requisito teleologico, che nel caso specifico potrebbe essere la tutela dell'ordine pubblico, della sicurezza nazionale, e la prevenzione dei reati. In conclusioni il principio di necessità viene individuato con il bisogno di raggiungere la proporzionalità tra i mezzi adottati e la finalità perseguita.

La sentenza finì con la condanna dell'Inghilterra, perché la conservazione dei dati personali a tempo indeterminato andava contro l'articolo 8 della CEDU, costituendo una violazione del diritto alla vita privata ed inoltre non rispettava il principio di proporzionalità richiesto.[8]

Un altro caso che evidenzia l'importanza del articolo 8 in materia di protezione dei dati personali e il caso *Alkaya vs. Turchia*. Durante questa sentenza si percepisce la tutela del articolo 8 prevista nei casi in cui le informazioni personali vengono rese pubbliche in assenza di un esplicito consenso da parte del interessato, anche qualora si trattasse di persone famose e pubbliche. Per motivi lavorativi queste persone subiscono di continuo intrusioni nella propria sfera privata da parte dei media, e quindi diventa problematico trovare un giusto equilibrio tra il diritto alla vita privata e il diritto di essere informati. Proprio in merito di tale tema tratta la sentenza della Corte di Strasburgo del 9 ottobre 2012 relativa al caso *Alkaya vs. Turchia*.

Yasemin Alkaya è un'attrice molto famosa nel mondo cinematografico e teatrale in Turchia. L'attrice turca subì un furto nella sua casa il 12 ottobre 2002. Data la fama dell'attrice, questa vicenda di cronaca venne riportata sui quotidiani locali e nazionali. Tra i quotidiani ce né una in particolare, il quotidiano nazionale "Aksam", il quale oltre a riportare l'accaduto, rende pubblico anche l'indirizzo di residenza di Alkaya. Motivo per cui l'attrice fa ricorso alla Corte domestica, Alta Corte di Zeytinburnu chiedendo un risarcimento danni di carattere materiale e morale nei confronti del quotidiano. Ma la sua richiesta viene respinta con la seguente motivazione da parte dell'Alta Corte: *"proprio per lo status di "persona famosa" non si può applicare la normativa nazionale sulla privacy, poiché in questo caso non c'è stato il carattere lesivo sul diritto riconosciuto. Si sostiene che a causa delle loro popolarità, persone come politici, sportivi e artisti sono soggetti a una maggiore attenzione e a una richiesta maggiore di informazioni da parte del pubblico. Sono soggetti quindi ad una privacy più esposta rispetto a quella della gente comune."*[9] Nonostante la normativa nazionale prevedesse che: *"Chiunque subisca un'interferenza illecita dei suoi diritti della personalità può intentare un'azione civile per chiedendo una somma di denaro a titolo di risarcimento e interesse per i danni morali subiti."*[10] Dunque indiffe-

[8] Sentenza della Corte EDU del 4 dicembre 2008 nel caso S. e Marper contro il Regno Unito.
[9] Sentenza della Corte EDU del 9 ottobre 2012 nel caso Alkaya vs. Turchia
[10] Ibidem.

rentemente dal fatto che si è persona pubblica o famosa, qualora venissero violati i diritti della personalità, sa ha la facoltà di agire civilmente per chiedere un risarcimento per i danni morali subiti.

Amareggiata della decisione dell'Alta Corte, che secondo l'attrice, ha adottato un comportamento discriminatorio nei suoi confronti, in quanto non ha applicato la norma sopra citata perché ritenuta una persona famosa a cui viene riservato un trattamento diverso rispetto ad un normale cittadino, in violazione del principio di non discriminazione ed equità.

Quindi l'attrice turca decide di rivolgersi alla Corte EDU, la quale espresse che l'indirizzo di residenza costituisce un dato strettamente personale che viene protetto dall'articolo 8 della CEDU. Così la Corte EDU:

"Si parla di tutela della persona e del suo domicilio, inteso come il luogo in cui avviene e sviluppa la vita privata e familiare. Per questo motivo, possono essere lesive di questo diritto anche le cose immateriali o intangibili che causano violazione della tranquillità di quel luogo. Nel caso di Alkaya, l'indirizzo di casa è un dato considerato sensibile e rientrante nelle informazioni personali del soggetto e quindi tutelate dalle norme preposte per questo. Non è ammissibile che una persona nota al pubblico non sia legittimata ad avere una tutela pari a quella prevista per i soggetti privati sconosciuti al grande pubblico."[11]

Se Alkaya chiedeva alla Corte EDU l'applicazione dell'articolo 8, il quotidiano nazionale "Aksam" basava la propria difesa sul articolo 10 – Libertà di espressione – della stessa Convenzione, che recita:

1. *"Ogni persona ha diritto alla libertà d'espressione. Tale diritto include la libertà d'opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera. Il presente articolo non impedisce agli Stati di sottoporre a un regime di autorizzazione le imprese di radiodiffusione, cinematografiche o televisive.*

2. *L'esercizio di queste libertà, poiché comporta doveri e responsabilità, può essere sottoposto alle formalità, condizioni, restrizioni o sanzioni che sono previste dalla legge e che costituiscono misure necessarie, in una società democratica, alla sicurezza nazionale, all'integrità territoriale o alla pubblica sicurezza, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, alla protezione della reputazione o dei diritti altrui, per impedire la divulgazione di informazioni riservate o per garantire l'autorità e l'imparzialità del potere giudiziario."*[12]

[11] Ibidem.
[12] Art. 10 – Libertà di espressione nella Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali.

Dunque la Corte EDU dovete trovare il giusto equilibrio tra il diritto al rispetto della vita privata previsto nell'articolo 8 della CEDU e la libertà di espressione garantita dall'articolo 10 della stessa Convenzione.
Il caso si concluse con l'affermazione da parte della Corte di Strasburgo della violazione dell'articolo 8 della Convenzione Europea. A tale conclusione si giunse valutando se l'informazione pubblicata sul quotidiano abbia apportato un contributo all'interesse pubblico. L'aver pubblicato l'indirizzo di residenza dell'attrice turca, nonostante questa persona fosse una figura pubblica, costituiva un semplice scoop giornalistico, senza perseguire la finalità principale della pubblicazione, ovvero quella di informare. Tutt'altro, rendendo pubbliche queste informazioni prettamente private poteva mettere in pericolo la sicurezza dell'attrice con riflessioni negative sulla sua sfera privata.

Un'altra definizione dell'articolo 8 venne data in occasione alla sentenza *Copland vs. il Regno Unito* del 3 aprile 2007,[13] riguardante la tutela della corrispondenza, la quale viene ampliata anche all'ambito lavorativo non solo in quello domestico.

Il caso riguarda la signora Copland, la quale svolgeva la mansione di assistente personale presso un college scozzese. Durante sei mesi le chiamate, le mail e la navigazione in Internet della signora Copland furono sottoposte al continuo monitoraggio da parte della struttura universitaria. L'assistente si lamentava della continua sorveglianza sul luogo e orario di lavoro e così decise di appellare alla Corte EDU invocando l'articolo 8 della CEDU. In risposta all'accaduto, il college espresse 2 motivazioni: la prima riguardava la garanzia di un alto livello di istruzione e per assicurare tale livello riteneva necessario esercitare un adeguato controllo sulle proprie strutture e sui suoi dipendenti, la seconda invece si riferiva alla protezione dei diritti e delle libertà altrui, e perciò riteneva necessario che l'università non venisse usata per scopi personali.

La sentenza della Corte si concluse con la valutazione dell'intrusione nella vita privata della signora Copland da parte del college scozzese ingiustificabile. In quanto la raccolta e la conservazione di dati personali riferiti all'utilizzo del telefono, della posta elettronica e del collegamento ad Internet da parte della dipendente costituivano un'ingerenza non prevista dalla legge (art.8 co.2) nella vita privata della signora Copland. Quindi la Corte ha riconosciuto la violazione dell'articolo 8 della Convenzione europea.

Caso più recente sempre sul tema del monitoraggio delle mail dei proppri dipendenti da parte del datore di lavoro fu il caso *Bărbulescu vs. Romania.*[14]

[13] Sentenza della Corte EDU del 3 aprile 2007 nel caso Copland vs. il Regno Unito.
[14] Sentenza della Grande Camera della Corte EDU del 5 settembre 2017 nel caso Bărbulescu vs. Romania.

Il signor Bogdan Mihai Bărbulescu, ingegnere di una società privata rumena, dopo esser stato licenziato dal proprio datore di lavoro per aver utilizzato l'account aziendale di posta elettronica a fini personali – e non per rispondere ai clienti, motivo per cui è stato creato tale account – sul posto e orario di lavoro, si è rivolto alla Corte nazionale in quanto ritiene che gli sia stato violato il diritto del rispetto alla vita privata previsto nell'articolo 8. Il Tribunale rumeno dette ragione al datore di lavoro. A quel punto l'ingegnere decise di fare appello alla Corte europea dei diritti dell'uomo. Diversamente dalla sentenza nel caso della signora Copland, questa volta ebbe un esito negativo per il signor Bărbulescu. Infatti, la Corte di Strasburgo, con la sentenza del 12 gennaio 2016, respinse la richiesta del signor Bărbulescu, in quanto in questo determinato caso non si ritenete esistente alcuna violazione dell'articolo 8 della CEDU. Tuttavia questo caso non si concluse qui, ma andò perfino dinanzi alla Grande Camera della Corte EDU, la quale capovolse l'esito della Corte EDU. Con la sentenza del 5 settembre 2017, la Grande Camera della Corte europea sui diritti dell'uomo stabilì che il monitoraggio della corrispondenza tramite posta elettronica aziendale dei propri dipendenti fosse legittima nel caso in cui l'utilizzo dell'account aziendale fosse utilizzato per scopi personali, solo se vengono ottemperati specifici parametri, quali l'esistenza di grave cause che legittimino il controllo, un'informazione preventiva, l'inesistenza di misure meno invasive.

Fin dall'apertura della sentenza, la Grande Camera ha dato un'interpretazione della connotazione di "vita privata" che si trova nella CEDU. Tale nozione si deve interpretare nel termine lato della parola, ovvero la vita privata di un individuo non si sviluppa soltanto nella sfera privata costituita dalle quattro mura domestiche, ma anche all'interno della società dove l'individuo svolge attività professionali, queste apportano notevoli contributi all'evoluzione della propria identità sociale. Ed è proprio sul luogo di lavoro che nascono le relazioni sociali. Quindi per la Grande Camera gli scambi di e-mail e le conversazioni personali durante lo svolgimento dell'attività professionale fanno parte del campo di tutela prevista dall'articolo 8 della CEDU. Nonostante tale tutela, i dipendenti non devono approfittare, ma devono impegnarsi al buon funzionamento aziendale e adempiere ai propri doveri professionali. Si tratta di trovare la giusta armonia tra il rispetto della vita privata dei dipendenti da parte del datore di lavoro e l'adempiere agli obblighi professionale da parte dei dipendenti per garantire il raggiungimento dello scopo aziendale, il tutto senza comprimere totalmente la vita privata sul luogo del lavoro.

Di diverso taglio fu il famoso caso *Uzun vs. Germania*[15] che si risolse con la sentenza della Corte EDU il 2 settembre 2010.
Il signor Uzun, abitante della Germania, fecce ricorso alla Corte federale di giustizia, in quanto riteneva che il fatto di essere stato osservato e controllato attraverso il GPS e l'im-

[15]Sentenza della Corte EDU del 2 settembre 2010 nel caso Uzun vs. Germania

piego della videosorveglianza continua per raccogliere dati, per poi impiegare tale materiale come prove nel processo penale contro di lui, andasse in violazione all'articolo 8 della Convenzione Europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Dopo il rifiuto del suo caso, appellò alla Corte federale costituzionale, e anche questa rigettò il caso sulla base del principio di necessità, esse infatti ha riconosciuto l'esistenza dell'ingerenza da parte delle autorità nella vita privata del ricorrente, ma tale ingerenza era proporzionata al grado di gravità delle azioni del ricorrente.

Il signor Uzun era sospettato per aver causato alcune esplosioni dalla cellula antiimperialista. Nei suoi confronti venne aperta un'indagine e per dimostrare ciò che si sospettava vennero utilizzati strumenti di sorveglianza sofisticati, quali il GPS, cimici, la videosorveglianza del palazzo dove ebbe la residenza e vennero intercettate le chiamate. L'impiego di questi strumenti nell'indagine furono precedentemente autorizzati. Tale procedura ebbe una durata di oltre un anno e si concluse con l'arresto del signor Uzun, con la condanna per tentato omicidio da scontare in prigione per una durata di 13 anni. Le prove che incastrarono il signor Uzun sono state ottenute grazie all'impiego del dispositivo GPS. Infatti si scopri l'intento di far esplodere diverse case di Parlamentari e perfino un consolato.

Dati gli esiti negativi da parte delle Corti nazionali a cui si appellò il ricorrente, egli decise di fare ricorso alla Corte europea dei diritti dell'uomo. Anche la Corte EDU, così come le Corti nazionali, riconobbe che la sorveglianza sugli spostamenti di un individuo con l'aiuto del monitoraggio della posizione GPS costituiva a tutti gli effetti un'invasione della vita privata, ma tale sorveglianza è stata precedentemente autorizzata dalla legge tedesca, la quale rilascia l'autorizzazione di un monitoraggio GPS soltanto in casi particolari, ovvero quando si ha a che fare con sospettati di crimini ritenuti di un determinato grado di gravità. Dunque la sorveglianza GPS poteva essere condotta solo sotto un controllo giudiziario. Per di più si osserva il rispetto del principio di necessità e proporzionalità della misure invasive adottate data la gravità dei crimini.

Inoltre la Corte richiama all'attenzione il comma 2 dell'articolo 8. Ovvero che le ingerenze nella vita privata sono state effettuate per salvaguardare la sicurezza pubblica, dal momento che il ricorrente era sospettato di tentati di omicidio.
La sentenza della Corte EDU si concluse con l'affermazione dell'inesistenza di alcuna violazione dell'articolo 8 della Convenzione.

La Corte di Strasburgo risolse innumerevoli casi in merito alla protezione dei dati personali, definendo ed interpretando ogni qualvolta l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali. Sempre sotto la tutela prevista dall'articolo 8 della CEDU fanno parte anche i dati personali riguardanti la

salute dell'individuo. Una conferma di ciò è la sentenza del 25 febbraio 1997 nel caso *Z. vs Finlandia.*[16]

L'articolo 8 compre un ampio raggio di tutela in tema di protezione dei dati personali, al suo interno viene collocata anche la protezione dell'immagine, come si pronunciò la Corte nella sentenza riguardante il caso *Von Hannover vs. Germania.*[17]

2.1.2 Il diritto alla privacy vs. il diritto alla protezione dei dati personali

Con l'avvento della gestione automatizzata dei dati e il sempre crescente numero di informazioni in circolazioni hanno posto in primo piano la problematica della protezione dei dati personali. Quindi la connotazione della privacy si può considerare una nozione in continuo mutamento, la quale necessiterà sempre di normativa aggiornate, che seguono il passo dell'evoluzione tecnologica. Ed è proprio l'utilizzo dei computer e la nascita della società d'informazione che segnano la necessità di una normativa che tuteli il diritto alla protezione dei dati personali.[18] Venne introdotta nel linguaggio giuridico europeo la nozione "data protection", protezione dei dati personali. Con l'espressione "Data protection" si intende: *"l'insieme di regole e strumenti giuridici ideati per proteggere i diritti, le libertà, e gli interessi degli individui i dati personali dei quali sono registrati, trattati e diffusi mediante computer da intrusioni illegali, e per proteggere le informazioni registrate nei confronti dell'alterazione, della perdita, della distruzione o della divulgazione non autorizzate, accidentali o intenzionali".*[19]

Nonostante la forte connessione tra il diritto alla privacy e il diritto alla protezione dei dati, tali diritti si devono considerare in maniera distinta. Come è stato detto in precedenza, il diritto alla privacy viene tutelato dall'articolo 8 della CEDU, mentre il diritto alla protezione dei dati venne concepito in seguito nell'era dell'informazione, quindi più recente. La prima disposizione sulla protezione dei dati rissale al 1970 adottata dal Land tedesco dell'Assia con validità territoriale soltanto in tale Stato. Tre anni dopo la Svezia adottò la prima normativa nazionale in materia di protezione dei dati al mondo. Successivamente, alla fine degli anni '80 seguirono Francia, Germania, Paesi Bassi e Regno Unito. Inizialmente l'adozione di una normativa in materia di protezione dei dati personali aveva lo scopo principale quello di controllare il trattamento dei dati personali da parte delle autorità pubbliche e delle grandi imprese. Col passare del tempo, la protezione dei dati ha subito continui mutamenti fino al punto di diventare un valore a sé, non classificabile come

[16] Sentenza della Corte EDU del 25 febbraio 1997 nel caso Z. vs. Finlandia.

[17] Sentenza della Corte EDU del 24 giugno 2004 nel caso Von Hannover vs. Germania.

[18] "Il diritto al rispetto della vita privata e il diritto alla protezione dei dati personali, sebbene strettamente connessi, sono diritti distinti." - Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018, cit. p. 20.

[19] Frits W. HONDIUS, *Emerging data protection in Europe*, Amsterdam, North-Holland Publishing Company, 1975.

il diritto al rispetto della vita privata previsto nell'articolo 8 della CEDU. Il diritto alla protezione dei dati viene riconosciuto dall'ordinamento giuridico dell'Unione Europea[20] come diritto fondamentale, ed in quanto tale, distinto dal diritto fondamentale alla privacy. E da qui scaturisce la necessità di individuare il rapporto che intercorre tra il diritto alla privacy e il diritto alla protezione dei dati.

Il punto focale che accomuna entrambi i diritti fondamentali è costituito dallo scopo comune di proteggere valori simili, ovvero la dignità umana e l'autonomia degli individui. Ambedue tutelano la sfera privata dove ciascun individuo possa sviluppare la propria personalità, possa esprimere liberamente i propri sentimenti, pensieri, la propria sessualità, il proprio culto e la propria religione, in altre parole la sfera privata costituisce un presupposto basilare per l'esercizio delle libertà fondamentali dell'individuo.

La differenza fra i due diritti viene individuata rispettivamente nella portata e nella formulazione. Il diritto alla privacy consiste in un divieto generale di ingerenza, assoggettato ad alcuni criteri di interesse pubblico che possono giustificare l'ingerenza in determinati casi, quali l'ordine pubblico e la sicurezza nazionale. Invece il diritto alla protezione dei dati venne letto come un'instaurazione di un sistema di controlli con l'intento di perseguire lo scopo di proteggere gli individui ogni volta che siano trattati i loro dati personali. Il trattamento dei dati deve seguire dei principi previsti dalla legge oltre che rispettare i diritti dell'interessato.[21] Inoltre il diritto alla protezione dei dati personali rispetto al diritto al rispetto della vita privata si riferisce ad una sfera più ampia, in quanto la sua applicabilità riguarda tutte le operazioni di trattamento dei dati personali indipendentemente dal fatto che ci sia o meno un impatto sulla vita privata. Quindi non è necessario dimostrare che sia stata violata la vita privata per far valere il diritto alla protezione dei dati personali. La protezione dei dati personali incorpora tutti i dati individuali a prescindere che si tratti di dati riguardanti esclusivamente la vita privata. Al contrario, il diritto al rispetto della vita privata ha un campo di applicazione ridotto a quello della sfera privata dell'individuo. La vita privata intesa in senso ampio, che comprende la parte intima di un individuo, le informazioni sensibili e riservate che potrebbero pregiudicare la percezione del pubblico nei confronti dell'interessato. La legge prevede l'intrusione delle autorità nella vita privata in violazione al diritto alla privacy nei casi eccezionali quali l'ordine pubblico e la sicurezza nazionale.[22]

[20] Gli strumenti adottati dal Consiglio d'Europa in materia di protezione dei dati verranno trattati nei paragrafi successivi del presente elaborato. Il primo strumento venne adottato nel 1981, la Convenzione n. 108 e per quanto riguarda uno strumento globale adottato dal CdE rissale al 1995 ed è la cosiddetta Direttiva Madre (Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera).

[21] Manuale sul diritto europeo in materia di protezione dei dati, edizione 2018

[22] Ibidem.

Un esempio per comprendere meglio tale distinzione tra il diritto alla vita privata e il diritto alla protezione dei dati può essere riferito nell'ambito lavorativo. Si supponga che il datore di lavoro tenga un registro in cui riporta i dati dei propri lavoratori, come i dati anagrafici, l'indirizzo e la retribuzione mensile. Il fatto che il datore di lavoro mantenga queste informazioni private dei propri dipendenti non costituisce un ingerenza nella vita privata, costituirebbe un'ingerenza se il datore di lavoro trasferisse a terzi tali informazioni private. Al contrario, il fatto di mantenere un registro con le informazioni relative ai dipendenti implica il trattamento dei dati, ergo, il datore di lavoro, in veste di responsabile del trattamento dei dati, è tenuto a rispettare le normative vigenti in materia di protezione dei dati personali.

2.1.3 La Convenzione n.108 del Consiglio d'Europa

La necessità di una normativa che regolasse l'uso dei computer e l'enorme quantità di dati personali contenuta nei registi elettronici spinse il Comitato dei ministri del Consiglio d'Europa, basandosi sull'articolo 8 della CEDU, ad adottare diverse risoluzioni[23] fino a redigere la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale ("Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"). Tale Convenzione viene adottata dal Comitato dei Ministri il 17 settembre 1980, e aperta alla firma il 28 gennaio 1981, a Strasburgo.

Convenzione che non assume la denominazione di Convenzione europea, ma solamente di Convenzione affinché possano aderire anche Stati non facenti parte del Consiglio d'Europa. Questo fatto rende la Convenzione una strumento giuridico a vocazione universale, e questo viene confermato dall'articolo 23 – "Adesione di Stati non membri" – della stessa:

[23] Consiglio d'Europa: adozione da parte del Comitato dei Ministri, il 26 settembre 1973, della risoluzione (73) 22 sulla protezione della privacy degli individui rispetto alle banche dati elettroniche nel settore privato; La Risoluzione assume la forma di una raccomandazione agli Stati membri, contenente un elenco di principi applicabili ai dati personali registrati in banche dati elettroniche nel settore privato. Tali principi riguardano:

a) la qualità delle informazioni;

b) le finalità delle informazioni;

c) i mezzi attraverso i quali le informazioni sono ottenute;

d) il periodo di conservazione dei dati;

e) il diritto all'informazione della persona interessata;

f) l'accesso alle informazioni;

g) la cancellazione e la rettifica delle informazioni;

h) le misure per prevenire gli abusi.

Dato che questa risoluzione tratta le banche dati esclusivamente nel settore privato, una anno più tardi, esattamente il 20 settembre 1974, il Comitato dei Ministri adotta la risoluzione (74) 29 sulla tutela della riservatezza delle persone in rapporto alle banche di dati elettroniche nel settore pubblico.
Anche questa risoluzione, come la precedente, assume la forma di una Raccomandazione ai Governi degli Stati membri, contenente un elenco di principi.

"Successivamente all'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa potrà invitare ogni Stato non membro del Consiglio d'Europa ad aderire alla stessa".[24]

Infatti il 10 aprile 2013 avviene l'adesione di Uruguay; il 17 giugno 2016 vi aderisce la Repubblica di Mauritius, sempre nel 2016 aderisce anche il Senegal; un anno dopo firmano la Convenzione anche Capo Verde, Marocco e Tunisia.

Tale atto è uno dei più importanti strumenti legali riguardante alla protezione dei dati personali, ed è l'unico giuridicamente vincolante a livello internazionale. Infatti nel preambolo viene posta l'attenzione sulla necessità di estendere la protezione dei dati in ogni dove per garantire i diritti e le libertà fondamentali di ciascun individuo, con riguardo anche al diritto al rispetto della vita privata previsto dal articolo 8 della CEDU. In seguito vengono riportate le precise parole che individuano tale bisogno:

"Gli Stati membri del Consiglio d'Europa, firmatari della presente Convenzione, considerando che scopo del Consiglio d'Europa è quello di realizzare una unione più stretta tra i suoi membri, nel rispetto in particolare della prevalenza del diritto nonché dei diritti umani e delle libertà fondamentali; considerando che è auspicabile estendere la protezione dei diritti e delle libertà fondamentali di ciascuno, e in particolare il diritto al rispetto della vita privata, tenuto conto dell'intensificazione dei flussi internazionali di dati a carattere personale oggetto di elaborazione automatica; riaffermando allo stesso tempo il loro impegno a favore della libertà d'informazione indipendentemente dalle frontiere; riconoscendo la necessità di conciliare i valori fondamentali del rispetto della vita privata e della libera circolazione delle informazioni tra i popoli".[25]

Dunque la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale viene adottata in risposta al bisogno di tutela per le persone nell'era dell'informazione. Lo sviluppo di nuovi mezzi di informazione e comunicazione da una lato hanno facilitato la vita delle persone, e dall'altro hanno reso gli individui vulnerabili di fronte alla comunità. Grazie ai computer e ai registri elettronici si aveva a disposizione un maggior numero di dati personali. Il semplice detenere dei dati personali implicava il loro trattamento. Il campo di applicazione della Convenzione n.108 riguarda tutti i trattamenti di dati personali effettuati sia nel settore privato che pubblico, e quindi anche i trattamenti effettuati da polizia e autorità giudiziaria.

[24] La Convenzione n. 108 in formato PDF, la si può consultare direttamente sul sito ufficiale del Garante per la protezione dei dati personali.
[25] Ibidem.

La Convenzione n.108 ha lo scopo di *"garantire, sul territorio di ciascuna Parte, ad ogni persona fisica, quali che siano la sua nazionalità o la sua residenza, il rispetto dei suoi diritti e delle sue libertà fondamentali, e in particolare del suo diritto alla vita privata, in relazione all'elaborazione automatica dei dati a carattere personale che la riguardano («protezione dei dati»)"*.[26]

Dunque la disposizione intende proteggere gli individui da abusi e regolamentare i flussi transnazionali dei dati.
Inoltre la Convenzione fissa dei principi che devono essere rispettati durante la raccolta e il trattamento dei dati, quali la correttezza, la liceità, la finalità del trattamento e la qualità dei dati. Tali principi costituiscono le fondamenta su cui si regge l'intera legislazione in materia di "Data Protection". La raccolta e il trattamento dei dati deve essere condotta ai sensi della legge, che ne autorizza il trattamento automatizzato. Tali dati devono essere trattati per scopi legittimi e specifici compatibili con la finalità di trattamento inizialmente prevista. La conservazione dei dati non deve oltrepassare il tempo necessario per il raggiungimento dell'obiettivo prefissato. Un ruolo fondamentale nel trattamento dei dati gioca il principio di correttezza, in base al quale i dati devono essere corretti e coerenti all'obiettivo preposto, inoltre non devono essere raccolti dati in quantità eccessiva, ma solo quelli necessari alla finalità perseguita.

Nella Convenzione 108 esiste anche un divieto riguardante il trattamento dei dati sensibili, ovvero la salute, la razza, l'orientamento sessuale e le opinioni politiche. Inoltre sancisce il diritto del cittadino ad ottenere informazioni in merito a quali dei suoi dati sono conservati ed eventualmente chiederne la rettifica se non corretti. È prevista la restrizione di alcuni diritti stabiliti nella Convenzione qualora ci siano interessi prevalenti, quali l'ordine pubblico o la sicurezza nazionale.
Per quanto riguarda il trasferimento dei dati verso paesi terzi, la Convenzione impone delle restrizioni qualora la legislazione del paese terzo non garantisca un tutela equivalente. Infine nella Convenzione è presente il principio della libera circolazione che non prevede il rilascio di un'autorizzazione, diversamente sarà stabilito dalla direttiva 95/46/CE.[27]

2.2 La Corte di giustizia dell'Unione europea

La Corte di giustizia dell'Unione europea (CGUE) viene istituita nel 1952 con la firma dei Trattati di Roma dei vari Stati membri e ha sede a Lussemburgo. Il suo ruolo è quello di interpretare il diritto dell'Unione europea con la finalità di garantire che tale diritto sia applicato in ugual misura in tutti gli Stati comunitari e risolvere le controversie giuridiche

[26] Articolo 1 della Convenzione n.108.
[27] B. SAETTA, articolo *Convenzione 108 del Consiglio d'Europa*,19 maggio 2018, pubblicato sul sito protezionedatipersonali.it

tra governi nazionali e istituzioni dell'UE. Possono fare appello alla CGUE anche singoli cittadini, organizzazioni o imprese nel caso in cui si sostenga di aver subìto una violazione dei loro diritti da parte di un'istituzione dell'Unione europea.

La Corte di giustizia dell'Unione europea è composta da due sezioni: la Corte di giustizia e il Tribunale.

1. La Corte di Giustizia a sua volta è formata da un giudice per ciascun paese membro più undici avvocati generali. Essa si occupa delle richieste di pronuncia pregiudiziale da parte dei tribunali nazionali e di alcuni ricorsi per annullamento e impugnazioni.[28]

2. Il Tribunale è formato da 47 giudici, che aumenteranno nel 2019 fino a 2 giudici per Paese, quindi 56 giudici. Il Tribunale apporta i suoi giudizi riguardanti il ricorsi di annullamento presentati dai privati, imprese ed in certi casi dai governi di paesi dell'UE. In poche parole il Tribunale si occupa di aiuti di Stati, diritto della concorrenza, commercio, agricoltura e marchi.[29]

In merito alla protezione dei dati la Corte di giustizia dell'Unione europea ha espresso il suo giudizio e ha apportato la sua interpretazione durante numerose sentenze. Tra queste si ricorda la causa *Google Spain SL e Google Inc. c. Agencia Espanola de Protección de Datos (AEDP), Mario Costeja Gonzales*,[30] sentenza della Corte (Grande Sezione) del 13 maggio 2014. La Corte ha risolto tale causa interpretando la Direttiva 95/46/CE, riconoscendo l'esistenza nell'UE del diritto alla cancellazione dei dati personali dai motori di ricerca su richiesta dell'interessato. Un'altra sentenza di fondamentale importanza per la materia di protezione dei dati riguarda l'accordo *Safe Harbour* tra l'Unione europea e Stati Uniti d'America. La causa in questione riguarda la denuncia di una persona fisica, *Maximillian Schrems*, i cui dati sono stati trasferiti dall'Unione europea verso gli Stati Uniti da parte del "Data Protection Commissioner". Nonostante il signor *Schrems* abbia presentato una

[28] Nelle pronunce pregiudiziali la CGUE esercita la sua funzione di interprete del diritto. *"I tribunali nazionali degli Stati membri devono assicurare la corretta applicazione del diritto dell'UE, ma i tribunali di paesi diversi potrebbero darne un'interpretazione differente. Se un giudice nazionale è in dubbio sull'interpretazione o sulla validità di una normativa dell'UE, può chiedere chiarimenti alla Corte. Lo stesso meccanismo può essere utilizzato per stabilire se una normativa o prassi nazionale sia compatibile con il diritto dell'UE".*
I ricorsi per annullamento, ovvero *"annullare atti giuridici dell'UE, se ritengono che un atto dell'UE violi i trattati o i diritti fondamentali, il governo di uno Stato membro, il Consiglio dell'UE, la Commissione europea o, in taluni casi, il Parlamento europeo, possono chiedere alla Corte di annullarlo. Anche i privati cittadini possono chiedere alla Corte di annullare un atto dell'UE che li riguardi direttamente."*
I ricorsi per omissione, ovvero *"assicurare l'intervento dell'UE, in talune circostanze, il Parlamento, il Consiglio e la Commissione devono prendere determinate decisioni. In caso contrario, i governi dell'UE, altre istituzioni dell'UE e, a certe condizioni, anche i privati cittadini o le imprese possono rivolgersi alla Corte".- https : //europa.eu/european − union/about − eu/institutions − bodies/court − justice¿t*

[29] Ibidem.

[30] Sentenza della Corte (Grande Sezione), 13 maggio 2014 nella causa C-131/12, Google Spain SL e Google Inc. c. Agencia Espanola de Protección de Datos (AEDP), Mario Costeja Gonzales.

denuncia al "Data Protection Commissioner", quest'ultimo si è rifiutato di istruire tale denuncia nei confronti di Facebook Ireland, in quanto il *social* trasferiva negli USA i dati personali dei propri utenti, che venivano conservati su server negli USA. Il signor *Schrems* facendo la denuncia si aspettava l'annullamento del trasferimento dei dati verso gli USA, in quanto riteneva l'inesistenza di un'adeguata protezione nei confronti dei dati personali dei cittadini comunitari. La Corte nazionale respinse tale denuncia ai sensi dell'accordo tra UE e USA, il cosiddetto "approdo sicuro". Questo spinse il signor *Schrems* a fare ricorso alla CGUE, la quale durante la sentenza del 6 ottobre 2015 dichiarò l'invalidità di tale accordo, ai sensi degli articoli 7 e 8 della Carta dei diritti fondamentali dell'Unione Europea e degli articoli 25 e 28 della Direttiva 95/46.[31]

2.3 L'ordinamento giuridico dell'Unione Europea riguardante la protezione dei dati

In seguito alla sua fondazione – avvenuta il 25 marzo 1957, quando sei stati[32] firmarono i Trattati di Roma – la Comunità economica europea seguì la scia del Consiglio d'Europa in merito al bisogno di redigere una legislazione che salvaguardasse i diritti fondamentali dell'uomo, in special modo una normativa che tutelasse i dati personali in un'epoca di continuo sviluppo tecnologico.

Agli inizi degli anni '70, la Commissione e il Parlamento Europeo, allarmati dalla competitività delle imprese americane nel settore dei computer e dei trattamenti dei dati, avvertirono il bisogno di una normativa armonizzata in tutti gli Stati membri, che avesse lo scopo di aiutare le società europee ad evolversi ed essere più competitivi in tali settori. Il primo documento della Commissione europea in merito rissale al 1973, e si tratta della una Comunicazione al Consiglio denominata "Community policy on data processing". Con questa Comunicazione la Commissione esprime l'urgente bisogno di adottare misure di supporto e favorevoli per lo sviluppo economico delle società europee, rendendole più competitive nel loro settore, inoltre viene sottolineata anche la necessità di misure che abbiano lo scopo di proteggere i cittadini.

Inizialmente il Consiglio europeo non sembra dare peso a tale Comunicazione. Il vero interesse verso queste tematiche si dimostrò nell'ottobre 1974 con l'incarico della Commissione giuridica del Parlamento europeo di predisporre una relazione relativa alla pro-

[31] Sentenza della Corte (Grande Sezione) del 6 ottobre 2015 nella causa C-362/14, Maximillian Schrems contro Data Protection Commissioner.

[32] I sei stati che hanno firmato il Trattato di Roma furono: Belgio, Francia, Germania, Italia, Lussemburgo, Paesi Bassi. Con il Trattato di Maastricht (1992) la Comunità europea (CE) costituì il "Primo pilastro" dell'azione dell'Unione europea (UE). La comunità europea giunge alla sua fine, in quanto con il Trattato di Lisbona (2009) viene assorbita dall'Unione europea. Per ulteriori approfondimenti consultare l'Enciclopedia Treccani

tezione dei diritti dell'uomo dinanzi alla continua evoluzione tecnologica nell'ambito del trattamento automatizzato dei dati. Tale relazione sarà il fondamento della Risoluzione del 1975 approvata dal Parlamento europeo in materia di protezione dei diritti dell'individuo di fronte al continuo sviluppo tecnologico nell'ambito dei dati automatizzati. In questa Risoluzione si sottolinea l'esigenza dell'adozione di una Direttiva sul tema di "automatic data processing". L'obiettivo della Direttiva deve essere quello di armonizzare le normative nazionali degli Stati membri e garantire massima tutela dei cittadini europei.

Nell'aprile 1976, in seguito a nessuna azione intrapresa da parte della Commissione europea e del Consiglio riguardante la Risoluzione del 1975, il Parlamento europeo adotta una seconda Risoluzione sempre in merito alla protezione dei diritti dell'individuo di fronte allo sviluppo tecnologico nel settore del trattamento automatizzato dei dati. Questa volta il Parlamento oltre a riaffermare quanto detto nella Risoluzione dell'anno prima, sollecitò la Commissione a redigere una proposta di legge al quanto prima. Inoltre, all'interno del Parlamento viene creata un'apposita Sottocommissione, la quale tra giugno 1977 e marzo 1979 redige una relazione in cui mostra l'operato delle legislazioni nazionali sia degli Stati membri della Comunità europea, che di alcuni Stati dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) e del Consiglio d'Europa.

Infatti a partire dal 1976 fino al 1979 la Commissione europea inizia ad occuparsi della materia. In primis cerca di capire l'intenzione degli Stati membri cercando di trovare un'armonizzazione delle rispettive legislazioni nazionali nell'ambito della protezione della privacy dei cittadini, data l'importanza di tale tematica per la Comunità economica europea. Durante questi tre anni la Commissione riscontra molte problematiche per quanto riguarda l'armonizzazione delle legislazioni nazionali di vari Stati membri in merito alla protezione della privacy. Fin da subito si evidenziarono le diversità per quanto riguarda le impostazioni della normativa in tema di protezione della riservatezza dei vari Stati. Un esempio è costituito dal fatto che alcuni Stati europei, come Austria, Danimarca e Norvegia nell'applicazione della legislazione sulla protezione della privacy vengono incluse anche le persone giuridiche oltre alle persone fisiche,[33] inclusione non necessaria per la Commissione. Tuttavia, altre alle divergenze, ci sono anche punti comuni come ad esempio l'approccio intraprendente che influenzò la maggior parte degli Stati membri. Infatti, molti Paesi tendevano a sviluppare strategie comune per arrivare a definire legislazioni nazionali simili. Seppur in alcuni Stati, come in Belgio, nei Paesi Bassi e nel Regno Unito non esistesse ancora una legge in tale materia, si discuteva riguardo una possibile proposta di legge. Non si può dire lo stesso per Italia e Irlanda, Paesi nei quali non vi era nemmeno l'ombra di un qualche minimo interesse ufficialmente documentato in merito alla protezione della privacy.

[33] Gloria GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*,Dordrecht, Springer, 2014.

In seguito alla relazione redatta dalla Sottocommissione, a maggio del 1979 il Parlamento europeo adotta una terza Risoluzione sulla protezione dei diritti dell'individuo di fronte al crescente sviluppo tecnologico nel settore del trattamento dei dati. La terza Risoluzione si presenta simile nei contenuti alle precedenti due Risoluzioni, l'unica sostanziale differenza sta nella generalità del trattamento dei dati, e non soltanto di quelli automatizzati. Inoltre il Parlamento europeo nella Risoluzione chiede alla Comunità economica europea un maggior interesse riguardo la materia di protezione della privacy e inoltre gli propone l'adesione alla Convenzione in lavorazione da parte del Consiglio d'Europa in quegli anni, ovvero la Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale, la cosiddetta Convenzione 108. In più, Il Parlamento europeo richiede nuovamente alla Commissione la predisposizione di una Direttiva con il fine di armonizzare le legislazioni nazionali degli Stati membri sulla tematica della protezione dei dati. Sempre nella presente Risoluzione sono inclusi alcuni principi che devono fungere da base per le future legislazioni nazionali in merito alla protezione dei dati. Tali principi comprendono sia gli obblighi del titolare del trattamento dei dati sia i diritti della persona di cui i dati vengono trattati, individuando anche l'ambito territoriale di tali diritti, infatti la legislazione si propone di proteggere i dati di quei cittadini che hanno residenza in uno Stato europeo. Inoltre sono previste delle autorità nazionali che vigilino sul rispetto della normativa sulla protezione dei dati.

Successivamente all'adozione della Convenzione 108 del Consiglio d'Europa – ritenuta adeguata in merito alla produzione di un grado di protezione dei dati armonizzato nell'intera Europa – la Commissione attraverso una Raccomandazione del 29 luglio 1981, sollecita a ratificare la Convenzione 108 da parte di tutti gli Stati facenti parte della Comunità economica europea entro la fine del 1982. Tale sollecitazione viene fatta anche da parte del Parlamento europeo con una nuova Risoluzione sulla protezione dei diritti dell'individuo di fronte al crescente sviluppo tecnologico nel settore del trattamento dei dati del marzo 1982, invocando un'adesione diretta della CEE alla Convenzione 108.

Ad ogni modo, il Parlamento si differenzia dalla Commissione, in quanto avverte il bisogno di predisporre norme comunitarie in merito alla protezione dei dati, sebbene esista la Convenzione del Consiglio d'Europa. Queste norme comunitarie devono sussistere sull'articolo 100 del Trattato che istituisce la Comunità economica europea (TCEE), il quale recita:

"Il Consiglio, deliberando all'unanimità su proposta della Commissione, stabilisce direttive volte al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che abbiano un'incidenza diretta sull'instaurazione o sul funzionamento del mercato comune.

L'Assemblea e il Comitato economico e sociale sono consultati sulle direttive la cui esecuzione importerebbe, in uno o più Stati membri, una modificazione nelle disposizioni legislative."[34]

Il tema trattato nell'articolo 100 del TCEE non è quello di interesse in questa sede, ma il Parlamento considera la disciplina in materia di protezione dei dati di vitale importanza per riuscire ad instaurare e far funzionare il *common market*.

2.3.1 La Direttiva 95/46/CE

Nel 1990 la Commissione europea presenta una Comunicazione relativa alla protezione dei dati personali – il Pacchetto del 1990. All'interno del Pacchetto, la Commissione include anche la proposta di una direttiva, la cosiddetta Direttiva "quadro" del Consiglio europeo *"concernente la protezione delle persone relativamente al trattamento dei dati personali dei dati"*,[35] con la finalità di armonizzare tutte le legislazioni nazionali in merito a tale materia. Questa finalità è dovuta la fatto che gli Stati membri hanno adottato legislazioni divergenti tra di loro, mettendo a rischio l'integrazione europea. Tale scopo perseguiva anche la Convenzione 108 del Consiglio d'Europa, alla quale aderì anche la Comunità economica europea, tuttavia alcune differenze sono continuate a persistere. Queste differenze riguardano soprattutto l'ambito di applicazione. Per esempio alcune norme si applicano sia alle persone fisiche sia alle persone giuridiche, altre invece solamente alle persone fisiche, problematica riscontrata precedentemente dalla Commissione. Inoltre in alcuni Stati dell'UE la normativa in merito alla protezione dei dati viene applicata soltanto per trattamenti automatizzati dei dati, non includendo quelli non automatizzati, altri Paesi invece includono nella disciplina entrambe le categorie di dati. Molte differenze si riscontrano anche nelle pre-condizioni del trattamento, ovvero quella parte del Trattamento nella quale vengono definiti gli obblighi di informazione durante la raccolta dati, oppure la modalità con cui verranno trattati i dati sensibili.

Dunque nella Proposta di Direttiva la Commissione intende raggiungere due fondamentali obbiettivi, ovvero la protezione della "privacy" delle persone relativamente al trattamento dei dati personali contenuti in archivi e la libera circolazione dei dati personali tra gli Stati membri. Richiamando ciò che è stato detto nella Risoluzione del 1982 del parlamento europeo, la Commissione nella proposta di Direttiva sottolinea la strumentalità di questa per l'instaurazione del mercato interno. In merito la Commissione del 1990 scrive: *"la diversità degli approcci nazionali e la mancanza di un sistema di protezione a livello della Comunità costituiscono un ostacolo al completamento del mercato interno. In effetti,*

[34] Trattato che istituisce la Comunità economica europea, articolo 100.

[35] Proposta di Direttiva del Consiglio concernente la protezione delle persone relativamente al trattamento dei dati personali. COM/90/314DEF – SYN 287 del 27/7/90.

se i diritti fondamentali delle persone interessate, in particolare il diritto alla vita privata, non sono garantiti a livello comunitario, si potrebbe assistere ad una limitazione del flusso transfrontaliero di dati, nel momento stesso in cui tale flusso è diventato indispensabile per le attività delle imprese e degli organismi di ricerca, come anche per la collaborazione fra le amministrazioni degli Stati membri nel quadro dello spazio senza frontiere. [...] un approccio comunitario in materia di protezione delle persone relativamente al trattamento dei dati personali si rivela altresì un'esigenza essenziale per lo sviluppo dell'industria dell'informatica e dei servizi telematici a valore aggiunto. La rapida introduzione di disposizioni armonizzate concernenti la protezione dei dati e della vita privata nel contesto delle reti digitali di telecomunicazione è indispensabile per la realizzazione del mercato interno delle apparecchiature e dei servizi di telecomunicazione. La penetrazione dell'informatica in tutte le sfere dell'attività economica e sociale e la costituzione di sistemi globali di comunicazione che facilitano l'integrazione di più attività rappresentano un'altra sfida che richiede una "protezione" adeguata ai rischi che potrebbero derivare da eventuali carenze tecniche o umane accidentali o volontarie. Un'efficace sicurezza dei sistemi d'informazione è un elemento essenziale per garantire una protezione effettiva della vita privata e per preservare l'integrità del patrimonio che costituiscono oggi i dati registrati e trasmessi sotto forma elettronica. Le politiche e i programmi comunitari per lo sviluppo delle industrie dell'informazione e delle telecomunicazioni e la realizzazione del mercato interno rischiano di essere fortemente ostacolati se non viene adottata una politica attiva di creazione, di sviluppo e di promozione di norme di sicurezza per i sistemi d'informazione. Dato che le telecomunicazioni permettono oggi gli scambi di dati su scala planetaria, la politica da adottare deve tenere conto di questa dimensione. Inoltre, è essenziale che le politiche nazionali in materia di sicurezza dell'informazione non diventino un ostacolo per la promozione dello sviluppo armonioso della Comunità e per le relazioni con i paesi terzi".[36] Per raggiungere gli obiettivi prefissati, la Proposta disciplina i seguenti punti fondamentali in merito alla protezione dei dati:

- Le condizioni di liceità del trattamento dei dati personali;
- I diritti dell'interessato;
- Il requisito della qualità dei dati;
- L'istituzione di un Gruppo di lavoro sulla protezione dei dati personali, ovverosia un organo con funzioni consultive.

Con riguardo alla Proposta è richiesta la consultazione del Comitato economico e sociale, il quale nell'aprile 1991 esprime il suo parere menzionando la necessità di inserire oltre alla tutela del diritto alla privacy anche la tutela dei diritti e libertà fondamentali della persona

[36] Ibidem.

previsti nella Convenzione 108 del Consiglio d'Europa.

Un anno dopo interviene anche il Parlamento europeo, che pur sostenendo la Proposta della Commissione del 1990, suggerisce dei mutamenti, tra cui l'ambito di applicazione della Proposta, che dovrebbe riguardare non tanto i dati personali "contenuti negli archivi" quanto la raccolta e il trattamento di essi.

Con l'entrata in vigore del Trattato di Maastricht (1 novembre 1993), la procedura per l'adozione della Proposta cambia. Infatti l'articolo 100 A del Trattato sull'Unione europea afferma: *"[...] Il Consiglio, deliberando in conformità della procedura di cui all'articolo 189 B e previa consultazione del Comitato economico e sociale, adotta le misure relative al ravvicinamento delle disposizioni legislative, regolamentari ed amministrative degli Stati membri che hanno per oggetto l'instaurazione ed il funzionamento del mercato interno".*[37] Facendo riferimento anche al citato articolo 189 B del Trattato che istituisce l'Unione europea apportando l'introduzione della procedura di co-decisione, che conferisce al Parlamento maggiori poteri nel processo decisionale,[38] mettendolo sullo stesso livello del Consiglio europeo in veste di co-legislatore.

Considerato questo, la Proposta della Commissione venne rivista e modificata tenendo conto dei suggerimenti del Comitato economico e sociale e del Parlamento. In primis viene modificato l'oggetto della Direttiva che diventa la tutela dei diritti e delle libertà fondamentali delle persone fisiche e particolarmente del diritto alla "privacy", con riguardo al trattamento dei dati personali. Inoltre vengono eliminate alcune differenze tra ambito privato ed ambito pubblico. In più viene data maggiore importanza alla disciplina del consenso dell'interessato.

In seguito a varie correzioni della Proposta da parte del Consiglio e compromessi escogitati da parte della Commissione per mettere d'accordo tutti gli Stati membri si arriva ad una comune convergenza a febbraio del 1995 e successivamente all'approvazione avvenuta il 24 ottobre 1995 della Direttiva 95/46/CE del Parlamento e del Consiglio europeo "relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati".

Come veniva specificato anche nella Proposta della Commissione del '90, le finalità della direttiva sono due: la prima è quella di uniformare le normative nazionali degli Stati membri in materia di protezione dei dati personali, garantendo il diritto alla privacy previsto anche dall'articolo 8 della Convenzione 108, e la seconda garantire un elevato grado

[37] Articolo 100 A del Trattato di Maastricht.
[38] Unione Europea - Trattati dell'UE

di sicurezza alla libera circolazione dei dati personali all'interno dell'UE.

La direttiva definisce nell'articolo 3 l'ambito di applicazione, che al contrario della Convenzione 108 è più vasto, in quanto tratta sia i dati personali automatizzati che quelli cartacei. Vi sono due esclusioni in merito alla sua applicazione (articolo 3, paragrafo 2), ovvero *"le disposizioni della presente direttiva non si applicano ai trattamenti di dati personali: - effettuati per l'esercizio di attività che non rientrano nel campo di applicazione del diritto comunitario [...] 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; - effettuati da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico."*[39]

Vengono stabiliti inoltre, i principi che si devono seguire affinché il trattamento dei dati personali venga considerato lecito, considerando di notevole rilievo il consenso dell'interessato. Sempre con riferimento all'interessato vengono definiti i suoi diritti, tra cui il diritto di accesso previsto dall'articolo 12 o il diritto di opposizione della persona interessata (artt.14). Viene disciplinato anche il trasferimento dei dati verso Paesi terzi al Capo IV nell'art 25 e seguenti. Il trasferimento dei dati verso Paesi terzi è possibile soltanto se il paese terzo garantisce un livello di protezione dei dati adeguato.

La Direttiva nell'articolo 28 pone in capo a ciascun Stato membro l'obbligo di formare a livello nazionale un'autorità indipendente con il compito di vigilare l'applicazione delle disposizioni di attuazione della Direttiva.

L'articolo 29 invece istituisce un Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali. Tale Gruppo, istituito a livello comunitario, "ha carattere consultivo ed indipendente", è composto da un rappresentante dell'autorità di controllo di ciascun Stato membro e da un rappresentante della Commissione. Il Gruppo di lavoro ha compiti ben precisi previsti dalla direttiva all'articolo 30.

Tale Direttiva, la cosiddetta Direttiva "madre", sarà la principale fonte normativa dell'UE in materia di protezione dei dati personali e la loro libera circolazione per oltre un ventennio, quando sarà completamente abrogata dal Regolamento generale sulla protezione dei dati, ufficialmente regolamento n. 2016/679.

[39] Direttiva 95/46/CE, Art.3 paragrafo 2.

2.3.2 Le fonti normative successive alla Direttiva 95/46/CE

Successivamente alla Direttiva "madre" vengono emanati ulteriori atti di diritto comunitario in merito alla protezione dei dati. Tra questi si ricorda il Regolamento (CE) N. 45/2001 del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati emanato il 18 dicembre 2000 ed entrato in vigore l'1 febbraio 2001. Tale Regolamento ha lo scopo di estendere la protezione dei dati personali anche al trattamento effettuato da organismi ed istituzioni comunitari. Inoltre esso soddisfa il bisogno di salvaguardare in tutti gli Stati membri un'applicazione coerente ed armonizzata delle disposizioni, in particolar modo della Direttiva 95/46/CE e della Direttiva 97/66/CE,[40] e altre disposizioni sulla materia della protezione dei dati personali, che intendono tutelare le libertà e i diritti fondamentali delle persone fisiche con riguardo al trattamento dei dati personali. Oltre a questo scopo, il Regolamento tutela anche la libera circolazione dei dati personali tra gli Stati membri e le istituzioni o gli organismi comunitari. Il perseguimento del duplice scopo viene raggiunto tramite la disposizione di norme vincolanti nei confronti delle istituzioni e degli organismi comunitari. Tali norme trovano applicabilità: *"ad ogni trattamento di dati personali effettuato da tutte le istituzioni e gli organismi comunitari purché esso avvenga nell'esercizio di attività che rientrano in tutto o in parte nel campo di applicazione del diritto comunitario."*[41]

Con il presente Regolamento viene istituito all'articolo 41 il Garante europeo della protezione dei dati (GEPD), *"un'autorità di controllo indipendente. [...] ha il compito di garantire il rispetto dei diritti e delle libertà fondamentali delle persone fisiche, segnatamente del diritto alla vita privata, riguardo al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari. [...] di sorvegliare e assicurare l'applicazione del presente regolamento e di qualunque altro atto comunitario relativo alla tutela dei diritti e delle libertà fondamentali delle persone fisiche riguardo al trattamento dei dati personali da parte di un'istituzione o di un organismo comunitario, e di fornire alle istituzioni e agli organismi comunitari nonché agli interessati pareri su tutte le questioni relative al trattamento dei dati personali."*[42]

Il 12 luglio 2002 il parlamento europeo e il Consiglio adottarono la Direttiva n. 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle

[40] La Direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. Tale direttiva fu adottata per integrare la Direttiva 95/46/CE per quanto riguarda il trattamento dei dati personali nel settore delle telecomunicazioni.

[41] Regolamento (CE) n.45/2001, Considerando 14 ripreso all'articolo 3.

[42] Il Regolamento (CE) n.45/2001, Capo V, articolo 41.

comunicazioni elettroniche. La sua adozione si ritiene necessaria come parte integrante della Direttiva 95/46/CE. Le finalità vengono definite fin dall'inizio nell'articolo 1:

1. *"La presente direttiva armonizza le disposizioni degli Stati membri necessarie per assicurare un livello equivalente di tutela dei diritti e delle libertà fondamentali, in particolare del diritto alla vita privata, con riguardo al trattamento dei dati personali nel settore delle comunicazioni elettroniche e per assicurare la libera circolazione di tali dati e delle apparecchiature e dei servizi di comunicazione elettronica all'interno della Comunità.*

2. *Ai fini di cui al paragrafo 1, le disposizioni della presente direttiva precisano e integrano la direttiva 95/46/CE. Esse prevedono inoltre la tutela dei legittimi interessi degli abbonati che sono persone giuridiche."*[43]

La direttiva inoltre definisce gli obblighi in capo ai fornitori di servizi di comunicazione elettronica accessibile al pubblico, che *"deve 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. Tenuto conto delle attuali conoscenze in materia e dei loro costi di realizzazione, dette misure assicurano un livello di sicurezza adeguato al rischio esistente"* - misure previste all'articolo 4. Sono sottolineati anche gli obblighi degli Stati di tutelare la privacy delle comunicazioni fatte con l'utilizzo della rete pubblica di comunicazione elettronica accessibili al pubblico, stabilito dall'articolo 5. Oltre agli obblighi sono presenti anche i diritti degli abbonati relativi alla fatturazione dettagliata sancito dall'articolo 7. Anche nell'ambito di questa direttiva il consenso ha un ruolo non da poco, in questo caso si riferisce alle comunicazioni indesiderate a scopo di commercializzazione diretta. Queste comunicazioni possono essere fatte solo previo consenso esplicito da parte degli abbonati ai sensi dell'articolo 13.

Tale direttiva viene considerata "figlia dello sviluppo tecnologico",[44] data la necessità di tutelare maggiormente i dati nell'era dell'informazione.

Un'altra fonte normativa dell'UE che tutela il diritto alla vita privata e famigliare e la protezione dei dati è la Carta dei diritti fondamentali dell'Unione europea, nominata anche Carta di Nizza, in quanto è stata proclamata a Nizza il 7 dicembre 2000. Successivamente viene riadattata una seconda volta nel dicembre 2007 a Strasburgo. In seguito all'entrata in vigore del Trattato di Lisbona,[45] avvenuta l'1 dicembre 2009, la Carta dei diritti fondamentali dell'Unione europea acquisisce lo stesso valore giuridico dei trattati, Infatti questo

[43] Il testo integrale della Direttiva 2002/58/CE consultabile sul sito ufficiale del Garante Privacy.

[44] M. SOFFIENTINI, *Privacy-protezione e trattamento dei dati*, Ipsoa Manuali, Assago, Wolters Kluwer, 2018.

[45] Il Trattato di Lisbona viene firmato il 13 dicembre 2007 ed entra in vigore l'1 dicembre 2009, modifica il trattato sull'Unione europea e il trattato che istituisce la Comunità europea, è composto dal Trattato dell'Unione europea (TUE) e dal Trattato sul Funzionamento dell'Unione europea (TFUE). Le novità

viene sancito dall'articolo 6 del presente Trattato, che recita: *"L'Unione riconosce i diritti, le libertà e i principi sanciti nella Carta dei diritti fondamentali dell'Unione europea del 7 dicembre 2000, adattata il 12 dicembre 2007 a Strasburgo, che ha lo stesso valore giuridico dei trattati."*[46] Nella Carta dei diritti fondamentali dell'Unione europea vengono stabiliti il diritto alla vita privata e famigliare e il diritto alla protezione dei dati rispettivamente dagli articoli 7 e 8. L'articolo 7 recita: *"Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni."*[47]

L'articolo 8 oltre a riconoscere il diritto di ciascun individuo alla protezione dei dati personali, stabilisce anche i principi che devono essere seguiti nell'operazione del trattamento dei dati, i diritti in capo alla persona interessata, e l'esistenza di un'autorità vigilante sul rispetto di tale regole. Infatti l'articolo 8:

1. *"Ogni individuo ha diritto alla protezione dei dati di carattere personale che lo riguardano.*
2. *Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni individuo ha il diritto di accedere ai dati raccolti che lo riguardano e di ottenerne la rettifica.*
3. *Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente."*[48]

Altra Direttiva che va menzionata in merito alla protezione dei dati personali è "la Direttiva n. 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006, concernente 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 modifica la Direttiva n. 2002/58/CE."[49] L'obiettivo di tale Direttiva viene definito all'articolo 1, comma 1: *"La presente direttiva ha l'obiettivo di armonizzare le disposizioni degli Stati membri relative agli obblighi, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, relativi alla conservazione di determinati dati da essi generati o trattati, allo scopo di garantirne la disponibilità a fini di indagine,*

del Trattato sono molteplici, tra cui vengono incrementati i poteri del Parlamento europeo, sono previsti nuovi provvedimenti per adeguare le Istituzioni europee all'allargamento dell'UE, l'organizzazione europea cambia completamente. "Esso evidenzia le materie che sono di competenza degli Stati membri e le materie nelle quali le decisioni sono prese direttamente dalle Istituzioni europee, in particolare dal Parlamento europeo e dal Consiglio, inoltre accresce la responsabilità democratica dell'Unione, rafforzando la Carta dei diritti fondamentali e consolidando lo stato di diritto". - Testo integrale del Trattato di Lisbona è consultabile sul sito ufficiale del Parlamento Europeo.

[46] Ibidem.

[47] Testo integrale della Carta dei diritti fondamentali dell'Unione europea è pubblicato sulla Gazzetta ufficiale delle Comunità europee - C 364/1.

[48] Ibidem.

[49] Op. cit. Supra note 44.

accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale."[50] La Direttiva definisce quale categorie di dati possono essere conservati all'articolo 5 ed all'articolo 6 viene individuato il periodo di conservazione dei dati che dev'essere maggiore alla durata di 6 mesi ed inferiore a quella di 2 anni.

Il 25 novembre 2009 viene adottata dal Parlamento europeo e dal Consiglio la "Direttiva n. 2009/136/CE, la cosiddetta Direttiva e-privacy, che ha apportato modifiche alla Direttiva n. 2002/22/CE, relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, alla Direttiva n. 2002/58/CE, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e al Regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori".[51] Lo scopo di questa Direttiva viene espresso nell'articolo 1 che così recita: *"[...] scopo della presente direttiva è garantire la disponibilità in tutta la Comunità di servizi di buona qualità accessibili al pubblico attraverso una concorrenza efficace e un'effettiva possibilità di scelta, nonché disciplinare i casi in cui le esigenze degli utenti finali non sono adeguatamente soddisfatte mediante il mercato. La direttiva contiene inoltre disposizioni riguardanti taluni aspetti delle apparecchiature terminali, comprese quelle volte a facilitare l'accesso per gli utenti finali disabili."*[52] La stessa stabilisce i diritti degli utenti e gli obblighi a carico dei fornitori di reti e servizi di comunicazione elettronica accessibili al pubblico.

Lo stesso giorno venne adottata la "Direttiva 2009/140/CE del Parlamento europeo e del Consiglio recante modifica delle direttive 2002/21/CE che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica, 2002/19/CE relativa all'accesso alle reti di comunicazione elettronica e alle risorse correlate, e all'interconnessione delle medesime e 2002/20/CE relativa alle autorizzazioni per le reti e i servizi di comunicazione elettronica".[53]

La Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, viene adottata in risposta alla necessità – avvertita dalla Commissione europea nel 2005, anno in cui fa una proposta di Decisione quadro – di uno strumento giuridico in merito alla protezione dei dati nell'ambito del Terzo pilastro (GAI – Giustizia e affari interni).[54] L'ambito di applicazione della Decisione quadro riguarda solo i trat-

[50] Direttiva n. 2006/24/CE, art. 1, co.1.
[51] Op. cit. Supra note 44.
[52] Direttiva n. 2009/136/CE Articolo 1.
[53] Op.cit. Supra note 44.
[54] "L'UE è fondata su una struttura a pilatri dal 1992 con il Trattato di Maastricht fino al 2007 con il Trattato di Lisbona. Nel Primo pilastro rientrano le Comunità europee, tra cui anche e soprattutto la CE; il Secondo pilastro consiste nella Politica estera e di sicurezza comune, o PESC; il Terzo pilastro è

tamenti transfrontalieri di dati personali, diversamente accadeva nell'ambito del Primo pilastro, dove la Direttiva "madre" garantiva un grado di protezione dei dati personali a livello nazionale.

2.4 Il Nuovo Pacchetto UE sulla protezione dei dati personali

In seguito ad un iter legislativo durato più di quattro anni il Parlamento europeo e il Consiglio approvano definitivamente il 27 aprile 2016 il "Nuovo Pacchetto europeo sulla protezione dei dati personali" contenente "il Regolamento UE n. 679/2016 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"[55] e la "Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la Decisione quadro 2008/977/GAI del Consiglio" . Il Regolamento entrerà in vigore 20 giorni dopo la pubblicazione, avvenuta il 4 maggio 2016, nella Gazzetta Ufficiale dell'Unione Europea, e tutti gli Stati membri saranno tenuti ad applicarlo direttamente a partire dal 25 maggio 2018, entro tale data la normativa nazionale dovrà essere adeguata al Regolamento in questione. Per quanto riguarda la Direttiva, essa entrerà in vigore il giorno dopo la pubblicazione in GUUE e obbliga gli Stati membri alla sua integrazione nel diritto nazionale entro il 5 maggio 2018.

L'obiettivo che si vuole raggiungere con il Pacchetto del 2016 lo si trova nel titolo della Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle Regioni: "Salvaguardare la privacy in un mondo interconnesso: Un quadro europeo della protezione dei dati per il XXI secolo." Dunque in un mondo in cui sembrerebbe che l'intera vita venga vissuta on-line, si avverte la necessità di tutelare il diritto alla privacy inteso come il diritto ad avere il controllo sui propri dati. Come sottolinea Stefano Rodotà: *"la tutela della privacy si è sempre più strutturata come diritto di ogni persona al mantenimento del controllo sui propri dati, ovunque essi si trovino, così riflettendo la nuova situazione nella quale ogni persona cede continuamente,*

costituito dalla GAI, Giustizia e affari interni. Mentre il Primo pilastro è caratterizzato dal "metodo comunitario", all'insegna dell'integrazione tra gli Stati membri, il Secondo e il Terzo sono contraddistinti da un "metodo intergovernativo", che comporta soltanto un rapporto di cooperazione tra gli Stati. La Direttiva 95/46/CE non si applica ai trattamenti di dati nell'ambito del Terzo pilastro, il quale inizialmente, in base al Trattato di Maastricht, include settori talvolta diversi tra di loro, come ad esempio asilo, immigrazione e cooperazione giudiziaria e di polizia in materia penale. Successivamente con il Trattato di Amsterdam si viene ad istituire lo "Spazio di Libertà, Sicurezza e Giustizia" (SLSG), e sposta il settore dell'asilo e dell'immigrazione dal Terzo al Primo pilastro. Nel Terzo, quindi, rimane fondamentalmente la cooperazione giudiziaria e di polizia in materia penale." - *http* : *//www.europarl.europa.eu/ftu/pdf/it/FTU*$_1$.1.3.*pdf*

[55] Il Regolamento UE n. 679/2016 consultabile direttamente sul sito ufficiale del Garante Privacy

e nelle forme più diverse, dati che la riguardano".[56] Il contesto di continua evoluzione tecnologica e globalizzazione che caratterizza la società dell'informazione rende sempre più difficile proteggere la propria sfera privata. Essa stessa ha assunto una connotazione diversa, infatti Rodotà definisce la sfera privata come: *"un luogo di scambi, di condivisione di dati personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita di cui altri possono appropriarsi o venire a conoscenza, ma interessa anche quelle in entrata, con le quali altri invadono quella sfera in forme sempre più massicce e indesiderate e così la modificano continuamente".*[57] Ecco che quindi ad un mutamento della società si devono adeguare anche gli strumenti giuridici che tutelano il diritto alla privacy. In risposta a tale necessità intervengono il Parlamento europeo e il Consiglio con il "nuovo Pacchetto sulla protezione dei dati personali".

In questa sede si svolgerà un'analisi approfondita del Regolamento Generale sulla Protezione dei Dati (RGPD)[58] applicabile oramai da un anno a questa parte in tutti i Paesi UE. In merito alla Direttiva (UE) 2016/680, essa non costituisce oggetto di analisi del presente elaborato, in quanto merita un approfondimento a parte dal momento che essa si riferisce a settori specifici, ovvero quello della giustizia, polizia e sicurezza, adopera regole e principi propri di questi settori. La sua origine è data dalla necessità, avvertita nei settori di cooperazione giudiziaria in materia penale e della cooperazione di polizia, di stabilire appunto regole specifiche sulla protezione della persone fisiche con riguardo al trattamento dei dati personali da parte delle Autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, incluse la salvaguardia e la prevenzione di minacce alla sicurezza pubblica, nel rispetto della natura specifica di tali attività. È un strumento inconfutabile, con il quale si impongono principi armonizzati, applicabili a tutte le operazioni di trattamento di dati svolte dalle Autorità pubbliche competenti al fine di prevenire, contrastare e reprimere i reati, nonché all'esecuzione delle pene.[59] Inoltre essa sostituisce la Decisione quadro 2008/977/GAI del Consiglio, che "ha un campo di applicazione limitato, in quanto si applica solo al trattamento transfrontaliero dei dati e non alle attività di trattamento effettuate dalla polizia e dalle autorità giudiziarie a livello strettamente nazionale". Questo fatto comporta seri problemi per le autorità competenti, dato che non è così immediato definire se il trattamento di dati in questione è a livello transfrontaliero oppure nazionale. In più la Decisione quadro, per la sua natura e per il suo contenuto, concede alle legislazioni degli Stati membri maggiore libertà in sede di esecuzione.

Questa Direttiva del Parlamento europeo e del Consiglio viene adottata per contrastare

[56] S. RODOTÀ, Il mondo nella rete. Quali i diritti, quali i vincoli. Roma, Laterza, 2014.
[57] Ibidem.
[58] In Inglese GDPR – General Data Protection Regulation.
[59] Op.cit. Supra note 44.

anche il fenomeno del terrorismo che caratterizza l'attuale contesto storico.

2.5 L'adeguamento della normativa nazionale al Nuovo Pacchetto protezione dati personali

La "Direttiva (UE) 2016/680 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la Decisione quadro 2008/977/GAI del Consiglio" è stata integrata in Italia con il D. Lgs. 18 maggio, n. 51 "Attuazione della 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 autorita' competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonche' alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio." Questo D. Lgs. è entrato in vigore l'8 giugno 2018 e ha dato attuazione alla direttiva UE n. 2016/680. Il D. Lgs. n. 51/2018 è suddiviso in otto Capi composti di cinquanta articoli, che si occupano di ambiti specifici della materia. Qualora si è in presenza di coincidenze con il Regolamento UE n. 2016/679 si rinvia alle disposizioni previste da quest'ultimo.

Per quel che riguarda il Regolamento UE n. 2016/679, oggetto di analisi in questa sede, nonostante esso sia applicabile e vincolante direttamente in tutti gli Stati membri senza richiedere una legge di recepimento nazionale, in Italia, il 4 settembre 2018 è stato pubblicato sulla Gazzetta Ufficiale il D. Lgs. 10 agosto 2018, n. 101 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del 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, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)". Nell'adeguare la normativa nazionale, ovvero il D. Lgs. n. 196/2003, il cosiddetto Codice della Privacy, al Regolamento generale sulla protezione dei dati, il legislatore deve considerare il diverso approccio in merito alla connotazione della privacy che intercorre nelle due normative, in quella nazionale ed in quella europea.

Innanzitutto il GDPR pone le sue fondamenta sul principio dell'*accountability*, ovvero il principio della responsabilizzazione, in base al quale viene stabilito l'obbligo per il titolare del trattamento dei dati personali di prevedere nell'adozione di misure adeguate tese all'attuazione dei principi di protezione dei dati previsti all'articolo 5 del Regolamento, inoltre esso dovrà dimostrare su richiesta dell'Autorità di controllo l'effettiva adozione

di tali misure.[60] Quindi il principio dell'*accountability* mette nelle mani del titolare del trattamento la responsabilità generale riguardante qualsiasi trattamento che egli stesso abbia effettuato o che altri suoi incaricati abbiano effettuato per conto suo, senza dettare i comportamenti da intraprendere e le misure da adottare. Non si può dire lo stesso per il Codice della Privacy, il quale prevedeva le misure da adottare affinché il titolare risulti uniformato. Il D. Lgs n. 101/2018 prevede delle misure di sicurezza riguardanti alcune categorie di dati, come i dati genetici, i dati attinenti alla salute, i dati biometrici, dettate dal Garante in un Provvedimento apposito che deve essere aggiornato ogni due anni. Di conseguenza, il nuovo Codice della Privacy viene modificato in maniera sostanziosa, perdendo parzialmente la sua centralità, considerato il fatto che le sue disposizioni dovevano essere lette in combinato disposto con quelle del Regolamento generale sulla protezione dei dati.

Il Legislatore nell'adeguatezza del Codice della Privacy al Regolamento europeo adotta una tecnica - redazionale "per novellazione", in quanto la maggior parte delle disposizioni nazionali erano da abrogare data la loro incompatibilità con le disposizioni previste dal GDPR, e la parte restante delle disposizioni codicistiche nazionali andavano modificate. Dunque dal perseguimento di questa tecnica redazionale in merito alla materia trattata, vengono evidenziati gli obiettivi che il Legislatore intende raggiungere, ovvero quello della chiarezza e della semplificazione, infatti, egli cerca di elidere i doppioni di alcune disposizioni presenti sia nella normativa nazionale che nel Regolamento, provvedendo alla loro abrogazione dal Codice e rimandando direttamente alle disposizioni europei in materia.[61]

[60] Si veda il Considerando 74 in merito alla responsabilizzazione del titolare del trattamento.
[61] Op. cit. Supra note 44.

Capitolo 3

Il Regolamento UE n. 2016/679 GDPR-RGDP

"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", altrimenti detto "Regolamento generale sulla protezione dei dati" o *"General Data Protection Regulation" (GDPR)*, è entrato in vigore lo scorso 24 maggio 2018 ed è applicabile in tutti gli Stati membri dal 25 maggio 2018, data in cui è stata mandata in pensione la Direttiva "madre" dopo aver ricoperto il ruolo della principale fonte normativa dell'UE in materia di protezione dei dati personali e la loro libera circolazione per oltre un ventennio.

3.1 La Struttura del RGPD

Il Regolamento generale sulla protezione dei dati è preceduto da 173 considerando aventi valore interpretativo – come ha sottolineato la Corte di Giustizia nella Sentenza del 14 dicembre 1989 riguardante il caso *Schweizerische Lactina Panchaud AG*[1] - ovvero qualora il testo non fosse chiaro o impreciso si può far riferimento ai considerando, ed è composto da 99 articoli suddivisi in XI Capi. La suddivisione dei Capi è la seguente:

Capo I "Disposizioni generali", strutturato in 4 articoli, dall'1 al 4;

Capo II "Principi", strutturato in 7 articoli, dal 5 al 10;

Capo III "Diritti dell'interessato", articolato in 5 Sezioni:

- Sezione 1: "Trasparenza e modalità", composta di un solo articolo, il 12;
- Sezione 2: "Informazione e accesso ai dati personali", composta di 3 articoli, dal 13 al 15;

[1] Sentenza del 14 dicembre 1989 riguardante il caso Schweizerische Lactina Panchaud AG, causa C-346/88.

- Sezione 3: “Rettifica e cancellazione”, composta di 5 articoli, dal 16 al 20;
- Sezione 4: “Diritto di opposizione e processo decisionale automatizzato relativo alle persone fisiche”, composta di 2 articoli, il 21 e il 22;
- Sezione 5: “Limitazioni”, composta di un solo articolo, il 23.

Capo IV “Titolare del trattamento e responsabile del trattamento”, articolato anche esso in 5 Sezioni:

- Sezione 1: “Obblighi generali”, composta di 8 articoli, dal 24 al 31;
- Sezione 2: “Sicurezza dei dati personali”, composta di 3 articoli, dal 32 al 34;
- Sezione 3: “Valutazione d’impatto sulla protezione dei dati e consultazione preventiva”, composta di 2 articoli, il 35 e il 36;
- Sezione 4: “Responsabile della protezione dei dati”, composta di 3 articoli, dal 37 al 39;
- Sezione 5: “Codici di condotta e certificazione”, composta di 4 articoli, dal 40 al 43;

Capo V “Trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali”, strutturato in 7 articoli, dal 44 al 50;

Capo VI “Autorità di controllo indipendenti”, articolato in 2 Sezioni:

- Sezione 1: “Indipendenza”, composta di 4 articoli, dal 51 al 54;
- Sezione 2: “Competenza, compiti e poteri”, composta di 5 articoli, dal 55 al 59;

Capo VII “Cooperazione e coerenza”, articolato in 3 Sezioni:

- Sezione 1: “Cooperazione”, composta di 3 articoli, dal 60 al 62;
- Sezione 2: “Coerenza”, composta di 5 articoli, dal 63 al 67;
- Sezione 3: “Comitato europeo per la protezione dei dati”, composta di 9 articoli, dal 68 al 76;

Capo VIII “Mezzi di ricorso, responsabilità e sanzioni”, strutturato in 8 articoli, dal 77 al 84;

Capo IX “Disposizioni relative a specifiche situazioni di trattamento”, strutturato in 7 articoli, dall’85 al 91;

Capo X “Atti delegati e atti di esecuzione”, strutturato in 2 articoli, il 92 e il 93;

Capo XI “Disposizioni finali”, strutturato in 6 articoli, dal 94 al 99.

Esso conferma i principi della Direttiva 95/46/CE, apportando delle modifiche in merito alla modalità di applicazione. A tal proposito il considerando 9 del regolamento sottolinea: *"Sebbene i suoi obiettivi e principi rimangano tuttora validi, la direttiva 95/46/CE non ha impedito la frammentazione dell'applicazione della protezione dei dati personali nel territorio dell'Unione, né ha eliminato l'incertezza giuridica o la percezione, largamente diffusa nel pubblico, che in particolare le operazioni online comportino rischi per la protezione delle persone fisiche. La compresenza di diversi livelli di protezione dei diritti e delle libertà delle persone fisiche, in particolare del diritto alla protezione dei dati personali, con riguardo al trattamento di tali dati negli Stati membri può ostacolare la libera circolazione dei dati personali all'interno dell'Unione. Tali differenze possono pertanto costituire un freno all'esercizio delle attività economiche su scala dell'Unione, falsare la concorrenza e impedire alle autorità nazionali di adempiere agli obblighi loro derivanti dal diritto dell'Unione. Tale divario creatosi nei livelli di protezione è dovuto alle divergenze nell'attuare e applicare la direttiva 95/46/CE."*[2]

Inoltre va sottolineata la differenza che persiste tra Direttiva e Regolamento. *"La Direttiva è un atto giuridico con il quale gli organi comunitari vincolano gli Stati membri destinatari per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi da adoperare di volta in volta."*[3] La direttiva viene definita anche nel Trattato sul Funzionamento dell'Unione europea all'articolo 288 comma 3: *"La direttiva vincola lo Stato membro cui è rivolta per quanto riguarda il risultato da raggiungere, salva restando la competenza degli organi nazionali in merito alla forma e ai mezzi."*[4] Mentre il comma 2 dello stesso articolo definisce il Regolamento: *"Il regolamento ha portata generale. Esso è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri."*[5] Quindi si evince la netta distinzione tra i due atti giuridici. In primis, la direttiva non è obbligatoria in tutti i suoi elementi; essa mira ad obbligare gli Stati membri al raggiungimento dell'obiettivo prefissato, senza interferire sui mezzi e sui metodi applicati, non si può dire lo stesso per il Regolamento, il quale deve essere messo in atto immediatamente senza che gli Stati membri adottino una normativa nazionale di recepimento. In secondo luogo il Regolamento è più dettagliato e completo rispetto alla Direttiva proprio per il motivo precedentemente illustrato. Il dettaglio si può osservare sia nelle definizioni dei significati dei termini sia nel definire i principi con grande cura.

[2] Considerando 9 del Regolamento generale sulla protezione dei dati.
[3] Definizione del termine "Direttiva" data dall'Enciclopedia "Treccani".
[4] Trattato sul funzionamento dell'Unione europea.
[5] Ibidem.

3.2 Il diritto alla privacy nel Regolamento UE 2016/679

Il diritto alla privacy nel Regolamento generale sulla protezione dei dati viene identificato con il diritto alla protezione dei dati, e questo fatto costituisce la novità del Regolamento. Tale differenza tra il GDPR e le precedenti fonti normative – in special modo l'articolo 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, l'articolo 1 della Convenzione 108, l'articolo 1 della Direttiva 95/46/CE ed infine gli articolo 7 e 8 della Carta dei diritti fondamentali dell'Unione europea – viene evidenziata all'articolo 1 del Regolamento, il quale recita:

1. *"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.*

2. *Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali.*

3. *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."*[6]

Mentre negli atti giuridici antecedenti il Regolamento si riscontrava sempre la stessa formula, ai sensi della quale la protezione dei dati personali veniva usata in veste di tutela dei diritti e delle libertà fondamentali, in speciale del diritto alla privacy, o come viene tradotto in italiano, del diritto alla vita privata, nel Regolamento si imbatte nell'espressione "il diritto alla protezione dei dati personali". Il diritto alla protezione dei dati non è un diritto in più che il Regolamento vuole tutelare oltre al diritto alla vita privata, ma è una sostituzione di quest'ultimo. Questa sostituzione ripercorre l'intero Regolamento, infatti la nozione di *"data protection"* viene utilizzata di frequente, al contrario la privacy viene menzionata poco, per esempio la nuova figura introdotta dal GDPR è il *Data Protection Officer* e non il *privacy Officer*, oppure la valutazione dell'impatto sulla protezione dati o la cosiddetta *"Data Protection Impact Assesment (DPIA)"*.
Il Regolamento intende tutelare la privacy, in special modo la protezione dei dati personali, in quanto diritto fondamentale della persona, come già veniva esplicitato all'articolo 8 della Carta dei diritti fondamentali dell'Unione europea. Questo si evince fin dal considerando 1 che si esprime in questi termini:

"La protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul

[6] Articolo 1 – Oggetto e finalità, GDPR.

funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano."

Per tutelare tale diritto, il Regolamento pone l'accento sui seguenti fattori:

1. Il rispetto dei principi e dei diritti delle persone: infatti agli articoli 5 e 6 il Regolamento fissa dei principi che ogni titolare del trattamento dei dati deve rispettare ed inoltre deve salvaguardare i diritti degli interessati previsti agli articoli 13 e seguenti fino all'articolo 22;

2. L'analisi del rischio e valutazione dell'impatto privacy: ogni titolare del trattamento deve predisporre un adeguato risk assesment, anche attraverso un apposito processo di valutazione, che valuti i rischi noti o che si possono rilevare e che tenga conto delle misure tecniche e organizzative fondamentali per conseguire lo scopo di mitigazione di tali rischi, ed in taluni casi consultare il Garante una volta fatta l'adeguata valutazione e stima dei possibili rischi;

3. La predisposizione del registro delle attività dei trattamenti: ai sensi dell'articolo 30, ogni titolare del trattamento dei dati deve disporre questo strumento fondamentale in cui si tengono tutti i trattamenti in essere che devono essere aggiornati di volta in volta che si presentano cambiamenti. Il registro deve avere forma scritta e deve essere esposto al Garante qualvolta lo richieda.

4. La sicurezza dei dati: sia il titolare che il responsabile del trattamento sono obbligati a ricorrere a misure tecniche e organizzative adeguate tali da garantire un livello di sicurezza idoneo al rischio del trattamento;

5. Il Responsabile della Protezione dei Dati (RPD) o *Data Protection Officer*(DPO): nuova figura introdotta dal Regolamento in merito al nuovo principio di responsabilizzazione, il cosiddetto principio dell'*accountability*, che evidenzia la natura responsabilizzante del Regolamento. I compiti del DPO vengono elencati all'articolo 39, tra questi rientra il compito di *"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."*[7] Inoltre la sua figura funge da punto di riferimento per gli interessati e per il Garante ogni qualvolta che si presentino questioni in merito all'applicazione del Regolamento.[8]

[7] GDPR – Articolo 39, lettera b).
[8] M. SOFFIENTINI, *Privacy-protezione e trattamento dei dati*, Assago, Ipsoa, 2018.

3.3 Una sintesi sugli argomenti trattati e le novità introdotte dal RGPD

Come già accennato nel paragrafo precedente, il Regolamento si basa su un approccio di responsabilizzazione in capo ai titolari e ai responsabili del trattamento dei dati personali. Queste figure sono tenute ad adottare opportuni criteri che prendano in considerazione i rischi derivanti da un certo trattamento dei dati personali per i diritti e le libertà degli interessati. Un altro principio inesistente negli atti giuridici che precedono il Regolamento, è il principio della *privacy by design*, ovvero salvaguardare la protezione de dati personali fin dalla fase di progettazione di un trattamento, in modo tale di riuscire a prevenire le varie problematiche che potrebbero nascere durante il trattamento.

Inoltre vengono introdotte norme specifiche e dettagliate riguardanti l'informativa e il consenso, vengono limitati i trattamenti automatizzati dei dati come la profilazione e i processi decisionali automatizzati. Il Regolamento pone le fondamenta per l'esercizio di nuovi diritti dell'interessato, come il diritto all'oblio (articolo 17) e il diritto alla portabilità dei dati (articolo 20). Ad esempio con l'esercizio del diritto all'oblio, l'interessato può chiedere la cancellazione dei dati qualora persistono delle condizioni previste dal presente Regolamento, come ad esempio non sono stati applicati i principi generali previsti oppure l'interessato si oppone legittimamente al loro trattamento. Una volta che l'interessato presenta la richiesta di cancellazione dei propri dati, il titolare del trattamento ha l'obbligo di comunicare tale richiesta di cancellazione a chiunque li stia trattando. Tale diritto può essere limitato in alcuni casi particolari, come ad esempio per finalità di garantire l'esercizio della libertà di espressione o il diritto alla difesa in sede giudiziaria o per tutelare un interesse pubblico, oppure a fini statistici o scientifici o storici, a patto che i dati siano in anonimato. Con il diritto alla portabilità dei propri dati personali è possibile trasferirli da un titolare del trattamento ad un altro, salvo alcune limitazioni, ad esempio non è possibile il trasferimento dei dati contenuti in archivi di interesse pubblico, ovvero le anagrafe.

In più il Regolamento adotta regole estremamente precise per quanto concerne il trasferimento dei dati verso Paesi terzi.[9] Inoltre come ambito territoriale di applicazione del presente atto giuridico non viene considerato soltanto il territorio dell'Unione europea. La sua applicabilità viene estesa a tutte le aziende, anche site al di fuori dell'UE, che offrono prodotti o/e servizi a cittadini residenti nel territorio dell'Unione.

Sempre dal GDPR viene introdotto l'istituto del "Sportello unico". In base a questo istituto, le imprese aventi stabilimenti in più Stati membri o che offrono servizi e/o prodotti in vari Paesi UE, per la risoluzione di questioni in merito all'applicazione e al rispetto del

[9] Per "Paese terzo" si intende Stato non appartenente all'Unione Europea.

presente Regolamento, hanno la possibilità di indirizzarsi ad un unico interlocutore, ovvero all'Autorità di protezione dei dati dello Stato dove risiede il loro stabilimento principale.

Inoltre vengono stabiliti criteri rigorosi e procedure da intraprendere nel caso in cui vengono violati i dati personali (*data breach*). Con il GDPR la notificazione preventiva prevista dalla Direttiva 95/46/CE viene abolita e al suo posto subentrano nuovi obblighi di tenuta di un registro dei trattamenti dei dati e dei *data breach* più l'obbligo di notificazione delle violazioni di dati personali (*data breach notification*). In merito alla notificazione delle violazioni di dati personali il considerando 85 pone l'accento sul fatto che la *data breach notification* non è obbligatoria in quanto essa è subordinata alla valutazione del rischio per gli interessati da parte del Titolare del trattamento. Infatti, dall'entrata in vigore del Regolamento UE n. 2016/679, *"tutti i titolari devono notificare all'Autorità di controllo le violazioni di dati personali di cui vengono a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati."* (Soffientini, 2018)

3.4 L'ambito di applicazione del Regolamento UE n. 2016/679

L'ambito di applicazione territoriale del presente regolamento viene individuato nell'articolo 3 dello stesso. Il quale introduce delle novità in merito all'applicazione del Regolamento UE n. 2016/679: innanzitutto, esso *"si applica al trattamento dei dati personali effettuato nell'ambito delle attività di uno stabilimento da parte di un titolare del trattamento o di un responsabile del trattamento nell'Unione, indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione."*

In merito a quanto affermato il considerando 22 fa chiarezza:

"Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un titolare del trattamento o responsabile del trattamento nel territorio dell'Unione dovrebbe essere conforme al presente regolamento, indipendentemente dal fatto che il trattamento avvenga all'interno dell'Unione. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica."

Dunque l'articolo 3 comma 1 stabilisce che, affinché venga applicato il Regolamento, è sufficiente che lo stabilimento del titolare o del responsabile sia ubicato nel territorio dell'UE.

Proseguendo nella lettura dell'articolo 3, al comma 2 viene individuata una seconda novità; ovvero che *"Il presente regolamento si applica al trattamento dei dati personali di interessati che si trovano nell'Unione, effettuato da un titolare del trattamento o da un responsabile del trattamento che non è stabilito nell'Unione, quando le attività di trattamento riguardano:*

a) *l'offerta di beni o la prestazione di servizi ai suddetti interessati nell'Unione, indipendentemente dall'obbligatorietà di un pagamento dell'interessato; oppure*

b) *il monitoraggio del loro comportamento nella misura in cui tale comportamento ha luogo all'interno dell'Unione."*

A proposito di questo, i considerando 23 e 24:

"Onde evitare che una persona fisica venga privata della protezione cui ha diritto in base al presente regolamento, è opportuno che questo disciplini il trattamento dei dati personali degli interessati che si trovano nell'Unione effettuato da un titolare del trattamento o da un responsabile del trattamento non stabilito nell'Unione, quando le attività di trattamento sono connesse all'offerta di beni o servizi a detti interessati indipendentemente dal fatto che vi sia un pagamento correlato. Per determinare se tale titolare o responsabile del trattamento stia offrendo beni o servizi agli interessati che si trovano nell'Unione, è opportuno verificare se risulta che il titolare o il responsabile del trattamento intenda fornire servizi agli interessati in uno o più Stati membri dell'Unione. Mentre la semplice accessibilità del sito web del titolare del trattamento, del responsabile del trattamento o di un intermediario nell'Unione, di un indirizzo di posta elettronica o di altre coordinate di contatto o l'impiego di una lingua abitualmente utilizzata nel paese terzo in cui il titolare del trattamento è stabilito sono insufficienti per accertare tale intenzione, fattori quali l'utilizzo di una lingua o di una moneta abitualmente utilizzata in uno o più Stati membri, con la possibilità di ordinare beni e servizi in tale altra lingua, o la menzione di clienti o utenti che si trovano nell'Unione possono evidenziare l'intenzione del titolare o del responsabile del trattamento di offrire beni o servizi agli interessati nell'Unione. È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un titolare del trattamento o di un responsabile del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al monitoraggio del comportamento di detti interessati, nella misura in cui tale comportamento ha luogo all'interno dell'Unione. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni per-

sonali."

In conclusione, l'articolo 3 al comma 3 sancisce che: *"Il presente regolamento si applica al trattamento dei dati personali effettuato da un titolare del trattamento che non è stabilito nell'Unione, ma in un luogo soggetto al diritto di uno Stato membro in virtù del diritto internazionale pubblico."*

Al riguardo, il considerando 25 apporta delucidazioni:

"laddove vige il diritto di uno Stato membro in virtù del diritto internazionale pubblico, ad esempio nella rappresentanza diplomatica o consolare di uno Stato membro, il presente regolamento dovrebbe applicarsi anche a un titolare del trattamento non stabilito nell'Unione."

Il motivo per cui viene estesa la disciplina europea in materia di protezione dei dati personali anche a Stati terzi lo si individua in alcune sentenze della Corte di giustizia dell'Unione europea (in modo particolare il famoso caso Google Spain SL, Google Inc. vs Agencia Espanola de Protección de Datos, Mario Costeja Gonzalez).[10] Infatti, la Corte di giustizia tenta di estendere l'applicazione della normativa UE anche a casi in cui i titolari non son stabiliti nel territorio dell'UE e il trattamento dei dati avviene in Stati terzi. Con il Regolamento UE n. 2016/679 si pone fine alla pretesa dei fornitori di servizi Internet *service provider* ubicati in Stati extra-UE, come gli Stati Uniti ad esempio, di sfuggire all'applicazione della disciplina europea nonché alla giurisdizione degli Stati UE, dato che la loro normativa in merito alla protezione dei dati offre garanzie inferiori in confronto a quello offerte dalla normativa europea.

Per garantire lo stesso livello di sicurezza e di tutela in merito alla protezione dei dati personali, ecco che il Regolamento generale sulla protezione dei dati impone alle imprese site in Stati terzi, ma che trattano dati di persone che si trovano nel territorio UE, il rispetto delle regole in esso stabilite.[11] Inoltre, al titolare o al responsabile del trattamento dei dati di queste imprese viene esplicitamente richiesta la designazione di un rappresentante nell'UE. Tale richiesta viene sancita dall'articolo 27 paragrafo 1:

"1. Ove si applichi l'articolo 3, paragrafo 2, il titolare del trattamento o il responsabile del trattamento designa per iscritto un rappresentante nell'Unione."

[10] La Corte di Giustizia dell'Unione europea si è pronunciata, in data 13 maggio 2014, in relazione al caso Google Spain SL, Google Inc. vs Agencia Española de Protección de Datos, Mario Costeja González (causa C131/12).

[11] Marinella FUMAGALLI MERAVIGLIA, *Le nuove normative europee sulla protezione dei dati personali*, in "Diritto comunitario e degli scambi internazionali", 2016.

Quindi il semplice fatto che un'impresa non sia situata in uno Stato membro non la esonera dall'applicazione del Regolamento generale sulla protezione dei dati. A seconda dell'attività svolta e dalla clientela servita dall'impresa stabilita in un Paese terzo, saranno i titolari del trattamento dei dati personali ad analizzare se sono tenuti a rispettare le regole stabilite dal GDPR o meno.

Per quanto concerne l'ambito soggettivo di applicazione, esso emerge fin dalla denominazione del Regolamento, infatti il presente regolamento è "relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali". Nella denominazione, oltre alla finalità del regolamento, viene individuato anche i soggetti a cui esso si applica, ovvero alle persone fisiche. Inoltre anche l'articolo 1 comma 2 definisce a chi viene indirizzato, esplicitandone il suo obiettivo di proteggere i diritti e le libertà fondamentali delle persone fisiche. Questo significa che tale disciplina non viene applicata alle società, ovvero alle persone giuridiche. Al riguardo il considerando 14:

"È opportuno che la protezione prevista dal presente regolamento si applichi alle persone fisiche, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali. Il presente regolamento non disciplina il trattamento dei dati personali relativi a persone giuridiche, in particolare imprese dotate di personalità giuridica, compresi il nome e la forma della persona giuridica e i suoi dati di contatto."

Nonostante sia prevista l'applicazione del Regolamento alle persone fisiche, questo non vuol dire che esso venga applicato a tutti i trattamenti di dati personali, infatti sono esclusi dal campo di applicazione del presente Regolamento i trattamenti di dati personali effettuato da un persona fisica per finalità esclusivamente personali. Una specificazione di quanto detto viene fornita dal considerando 18:

"Il presente regolamento non si applica al trattamento di dati personali effettuato da una persona fisica nell'ambito di attività a carattere esclusivamente personale o domestico e quindi senza una connessione con un'attività commerciale o professionale. Le attività a carattere personale o domestico potrebbero comprendere la corrispondenza e gli indirizzari, o l'uso dei social network e attività online intraprese nel quadro di tali attività. Tuttavia, 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."

Un altro caso in cui non trova applicazione il Regolamento UE n. 2016/679 è riferito ai

dati personali delle persone decedute.[12] Il Regolamento prevede che gli Stati membri sono liberi ad adottare norme inerenti al trattamento dei dati delle persone decedute. La sua non applicabilità riguardante il trattamento dei dati delle persona decedute ripercorre anche nei considerando 158 e 160. Il considerando 158 menziona il trattamento dei dati personali a fini di archiviazione affermando l'applicazione del Regolamento con esclusione del trattamento dei dati di persone decedute. Sempre nel considerando 158 vengono sottolineati gli obblighi legali ai quali sono tenuti ad adempiere le autorità pubbliche o gli organismi pubblici o privati che tengono registri di interesse pubblico. Mentre il considerando 158 si riferisce al trattamento dei dati personali a fini di archiviazione, il considerando 160 sottolinea l'applicabilità del Regolamento ai trattamenti dei dati a fini di ricerca storica, tenendo conto dell'esclusione dal campo di applicazione il trattamento dei dati delle persone decedute.

3.5 I Principi

Il Capo II del Regolamento UE n. 2016/679 si occupa dei principi che sono alla base della materia in esame. Facendo riferimento al considerando 9, i principi e gli obiettivi della direttiva 95/46/CE rimangono validi. Tali principi vengono esposti in 7 articoli, dall'articolo 5 all'articolo 11. L'articolo 5 elenca tutti i principi che fungono da fondamenta per l'intera disciplina. Data la sua importanza, verrà riportata di seguito:

1. *"I dati personali sono:*

    a) *trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»);*

    b) *raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»);*

    c) *adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);*

    d) *esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»);*

    e) *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; i dati personali possono essere conservati per periodi più lunghi a condizione*

[12] GDPR considerando 27.

che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) *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 («integrità e riservatezza»).*

2. *Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).”*

Al riguardo il considerando 39 chiarisce che il trattamento dei dati affinché sia lecito e corretto, *“devono essere trasparenti per le persone fisiche le modalità con cui sono raccolti, utilizzati, consultati o altrimenti trattati dati personali che le riguardano nonché la misura in cui i dati personali sono o saranno trattati.”* Dunque viene sottolineato anche il principio della trasparenza, in base al quale *“le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro.”* Inoltre, viene rilevata l'importanza dell'informativa recante le finalità del trattamento, che devono essere esplicite e legittime al momento della raccolta dei dati, i rischi che comporta, le norme che regolano tale trattamento, i diritti dell'interessato e le garanzie, ed infine le modalità di esercizio dei diritti degli interessati in merito al trattamento. In più, *"I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento"*. Di conseguenza, i titolari del trattamento dei dati devono limitare la conservazione di tali dati ad un minor tempo possibile e sufficiente al raggiungimento della finalità perseguita. Una volta raggiunta la finalità prefissata, il titolare del trattamento ha l'obbligo di prevedere alla cancellazione dei dati o ad una verifica periodica di essi. Qualora si è in presenza di dati personali inesatti, il titolare ha l'obbligo di adottare misure adeguate al riguardo, procedendo in taluni casi alla rettifica dei dati inesatti o addirittura alla loro cancellazione. In conclusione, *“I dati personali dovrebbero essere trattati in modo da garantirne un'adeguata sicurezza e riservatezza, anche per impedire l'accesso o l'utilizzo non autorizzato dei dati personali e delle attrezzature impiegate per il trattamento.”*[13]

Per quanto concerne il paragrafo 2 dell'articolo 5 riferito al principio della responsabilizzazione, il considerando 74[14] recita:

[13] GDPR, considerando 39.

[14] Considerando 74 precedentemente accennato al paragrafo 2.6. “L'adeguamento della normativa nazionale al Nuovo Pacchetto sulla protezione dei dati personali”.

"È opportuno stabilire la responsabilità generale del titolare del trattamento per qualsiasi trattamento di dati personali che quest'ultimo abbia effettuato direttamente o che altri abbiano effettuato per suo conto. In particolare, il titolare del trattamento dovrebbe essere tenuto a mettere in atto misure adeguate ed efficaci ed essere in grado di dimostrare la conformità delle attività di trattamento con il presente regolamento, compresa l'efficacia delle misure. Tali misure dovrebbero tener conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché del rischio per i diritti e le libertà delle persone fisiche."

L'articolo 5 della normativa europea è molto simile nel testo all'articolo 11 del Codice della Privacy precedente le modifiche apportate dal D. Lgs. n. 101/2018.

3.5.1 Il Principio di liceità, correttezza e trasparenza

Il principio di liceità viene espresso all'articolo 6 attraverso un elenco di condizioni che deve rispettare il trattamento affinché esso possa essere considerato lecito. Per prima condizione si trova il consenso dato da parte dell'interessato al trattamento dei propri dati personali per una o più specifiche finalità. Il consenso ha un ruolo centrale nel Regolamento. A proposito del consenso il considerando 40 esplicita:

"Perché sia lecito, il trattamento di dati personali dovrebbe fondarsi sul consenso dell'interessato o su altra base legittima prevista per legge dal presente regolamento o dal diritto dell'Unione o degli Stati membri, come indicato nel presente regolamento, tenuto conto della necessità di ottemperare all'obbligo legale al quale il titolare del trattamento è soggetto o della necessità di esecuzione di un contratto di cui l'interessato è parte o di esecuzione di misure precontrattuali adottate su richiesta dello stesso."

A seguire vengono elencate le cause per cui il trattamento è lecito nonostante la mancanza del consenso dell'interessato. Questi sono:

b) *"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;*

c) *il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;*

d) *il trattamento è necessario per la salvaguardia degli 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 o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore."*

Con riguardo all'elencazione delle casistiche la cui presenza rende il trattamento lecito si vedano i considerando dal 40 al 50.

Riprendendo il tema del consenso, in special modo le condizioni per il consenso, queste vengono trattate all'articolo 7 del Regolamento europeo e costituiscono una novità. L'articolo 7 illustra appunto, quali sono le condizioni alle quali l'interessato può manifestare e revocare il proprio consenso. In speciale, *"se il consenso dell'interessato è prestato nel contesto di una dichiarazione scritta che riguarda anche altre questioni, la richiesta di consenso è presentata in modo chiaramente distinguibile dalle altre materie, in forma comprensibile e facilmente accessibile, utilizzando un linguaggio semplice e chiaro. Nessuna parte di una tale dichiarazione che costituisca una violazione del presente regolamento è vincolante."*[15] Inoltre, al paragrafo 3 viene riconosciuto all'interessato il diritto di revocare il consenso, che può essere esercitato in qualsiasi momento senza compromettere la legittimità del trattamento basata sul consenso prima della revoca. Al riguardo va sottolineata l'importanza dell'informativa sul trattamento che il titolare ha l'obbligo di dare all'interessato ancor prima di raccogliere i suoi dati e di avere il suo consenso.

Di fondamentale importanza è anche il paragrafo 1 del presente articolo, in base al quale viene stabilito l'onere in capo al titolare di dimostrare che l'interessato ha prestato il suo consenso al trattamento dei suoi dati personali.

Oltre a dover essere legittimo, il trattamento deve essere corretto, ovvero lo svolgimento del trattamento deve avvenire in modo onesto e leale. Per verificare se si è rispettata o meno la correttezza del trattamento si prendono in considerazione le sue conseguenze sulla persona interessata.

Ulteriormente il trattamento deve essere trasparente in base al principio di trasparenza. *"Il principio della trasparenza impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro. Tale principio riguarda, in particolare, l'informazione degli interessati sull'identità del titolare del trattamento e sulle finalità del trattamento e ulteriori informazioni per assicurare un trattamento corretto e trasparente con riguardo*

[15] Articolo 7, paragrafo 2 del Regolamento UE n. 2016/679.

alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano".[16]

3.5.2 Il Principio di finalità

Il principio di finalità viene previsto all'articolo 5 lettera b), in base al quale le finalità del trattamento devono essere determinate, esplicite e legittime ed inoltre i dati personali devono essere trattati in modo compatibile con le finalità prefissate.

A tal riguardo il considerando 50 sancisce che i successivi trattamenti dei dati personali raccolti devono essere compatibili con le finalità prestabilito inizialmente.
Per approfondire tale principio bisogna capire cosa si intende per finalità determinate, esplicite e legittime. Innanzitutto, con il termine "determinate" si intende che le finalità devono essere specificate. Per esplicite si intende che le finalità devono essere espresse in modo chiaro. E con l'espressione legittime si fa riferimento alla liceità del trattamento, trattato all'articolo 6.

3.5.3 Il Principio di adeguatezza, pertinenza, non eccedenza

In base all'articolo 5 lettera c) *"i dati personali sono adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»);"*

Fin da subito si nota la stretta correlazione tra questo principio e il principio di finalità, dato che i dati raccolti devono essere pertinenti alla finalità prefissata, ovvero i dati raccolti servono alla finalità dichiarata e non sono superflui rispetto ad essa. Infatti con il termine "pertinente" ci si riferisce proprio ai dati che servono al raggiungimento della finalità predefinita. Inoltre questi dati devono essere "adeguati", ovvero necessari per raggiungere la finalità dichiarata. Ed infine i dati raccolti devono essere "non eccedenti", concernente al principio di necessità o al cosiddetto "principio di minimizzazione dei dati" previsto dal Codice della Privacy prima delle modifiche apportate dal D. Lgs. n. 101/2018. Tale principio stabilisce che il titolare del trattamento deve raccogliere i dati ritenuti indispensabili per il perseguimento delle finalità dichiarate.

3.5.4 Il Principio di esattezza e aggiornamento

Il principio di esattezza e aggiornamento viene individuato all'articolo 5 lettera d) ed esige che i dati vengano verificati non soltanto al momento della loro raccolta, bensì anche successivamente con opportuni aggiornamenti periodici. E tali aggiornamenti devono essere effettuati dal titolare del trattamento, il quale prevede alla predisposizione di misure

[16] Considerando 39, GDPR.

di rilevamento apposite al conseguimento di tale fine. Il nome stesso del principio fa riferimento al fatto che i dati devono essere esatti, ovvero attendibili, ed aggiornati, cioè attuale.[17]

3.5.5 Il Principio di conservazione dei dati

"I dati personali sono 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; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

Dunque in base a tale principio i dati devono essere conservati in maniera tale da permettere l'identificazione dell'interessato solo per il tempo necessario al raggiungimento delle finalità per le quali sono stati raccolti. La normativa prevede anche un'unica eccezione in cui i dati personali raccolti posso superare tale durata, e questa è l'archiviazione per motivi di interesse pubblico, di ricerca scientifica o storica o a fini statistici.

3.5.6 Il Principio di sicurezza adeguata

Il principio di sicurezza adeguata sancisce il fatto che il titolare del trattamento dei dati personali deve ha il dovere di adottare misure tecniche e organizzative adeguate in modo tale da garantire una sicurezza adeguata dei dati personali. I dati devono essere protetti da trattamenti non autorizzati o illeciti, dalla loro perdita o distruzione o da danni accidentali, tale protezione implica la salvaguardia dell'integrità dei dati. Con riguardo alla "violazione dei dati personali" si fa riferimento alla definizione data all'articolo 4, comma 1 n. 12 del Regolamento europeo, che recita: *"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;* Questa definizione di "violazione dei dati" viene precisata al considerando 85, sottolineando l'importanza dell'adeguatezza e della tempestività delle misure adottate in merito alla violazione dei dati. Infatti se non vengono impiegate misure adeguate con una certa immediatezza per contrastare la violazione dei dati, questa può provocare danni sia materiali che immateriali alle persone fisiche.

Il Regolamento generale sulla protezione dei dati prevede una serie di garanzie di sicurezza, che vengono elencate all'articolo 32. Tra queste garanzie di sicurezza viene menzio-

[17] Principio previsto anche nel Codice della Privacy antecedente le modifiche apportate dal D. Lgs. n. 101/2018 all'articolo 11, comma 1, lett. c).

nata la pseudonimizzazione. Inoltre viene posta l'attenzione sull'importanza della valutazione dei rischi attraverso la *data protection impact assesment (DPIA)*, la quale permette al titolare di individuare i rischi specifici del trattamento, affinché gli consenta di adottare misure di sicurezza adeguate in merito.

3.5.7 *Data protection by design* e *data protection by default*

L'articolo 25, comma 1 del Regolamento UE n. 2016/679 disciplina i principi della *privacy by design*, il quale:

"Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la pseudonimizzazione, volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati."

Con l'espressione *"data protection by design"* si intende la protezione dei dati fin dalla fase di progettazione di un trattamento di dati personali, ovvero il titolare del trattamento è tenuto a predisporre misure tecniche e organizzative atte a garantire un livello maggiore di riservatezza dei dati, altrimenti adoperare un trattamento minimizzante del loro uso. Come menzionato nel paragrafo precedente, una tecnica adatta all'attuazione efficace dei principi di *data protection*, tendente a minimizzare l'uso è la pseudonimizzazione.[18]

L'attuazione di tecniche adeguate per il rispetto dei principi di protezione dei dati introduce il concetto di *"data protection by default"*, al quale viene dedicato il comma 2

[18]"La pseudonimizzazione implica tre elementi:

- l'assenza di identificabilità diretta del soggetto interessato («trattamento dei dati personali in modo tale che i dati non possano essere più attribuiti ad un interessato specifico senza l'utilizzo di informazioni aggiuntive»);
- l'adozione di misure di sicurezza ulteriori da aggiungere alla pseudonimizzazione («a condizione che tali informazioni aggiuntive siano conservate separatamente»);
- l'incorporazione della pseudonimizzazione nella "privacy-by-design" («e 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 consente di raccogliere dati diversi ma relativi allo stesso soggetto, senza che di esso si conosca l'identità in modo diretto. Così, anche se il soggetto rimane identificabile, devono comunque sussistere motivi legittimi per effettuare l'identificazione, perchè i dati personali devono essere "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" ai sensi dell'articolo 5, comma 1, lettera b) del Regolamento generale sulla protezione dei dati. Al riguardo si vedano anche il considerando 28 e l'articolo 32 del GDPR."

dell'articolo 25 del GDPR:

"Il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare, dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica."

Tale protezione dei dati ha un ruolo fondamentale soprattutto quando si ha a che fare con trattamenti automatizzati, in quanto la protezione dei dati personali è garantita da impostazioni predefinite.

Come si evince da quanto appena detto che lo scopo della *data protection by design* è quello di rendere i trattamenti conformi al Regolamento europeo sulla protezione dei dati personali, invece la *data protection by default* persegue l'obiettivo di proteggere i trattamenti automatizzati da violazioni, quali l'accesso non consentito e trattamenti per finalità diverse da quelle dichiarate al momento della raccolta dei dati, con l'adozione di impostazioni predefinite, appunto di "default". Tali impostazioni predefinite consentono il rispetto del Regolamento generale sulla protezione dei dati.

In merito, il considerando 78:

"La tutela dei diritti e delle libertà delle persone fisiche relativamente al trattamento dei dati personali richiede l'adozione di misure tecniche e organizzative adeguate per garantire il rispetto delle disposizioni del presente regolamento. Al fine di poter dimostrare la conformità con il presente regolamento, il titolare del trattamento dovrebbe adottare politiche interne e attuare misure che soddisfino in particolare i principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita. Tali misure potrebbero consistere, tra l'altro, nel ridurre al minimo il trattamento dei dati personali, pseudonimizzare i dati personali il più presto possibile, offrire trasparenza per quanto riguarda le funzioni e il trattamento di dati personali, consentire all'interessato di controllare il trattamento dei dati e consentire al titolare del trattamento di creare e migliorare caratteristiche di sicurezza. In fase di sviluppo, progettazione, selezione e utilizzo di applicazioni, servizi e prodotti basati sul trattamento di dati personali o che trattano dati personali per svolgere le loro funzioni, i produttori dei prodotti, dei servizi e delle applicazioni dovrebbero essere incoraggiati a tenere conto del diritto alla protezione dei dati allorché sviluppano e progettano tali prodotti, servizi e applicazioni e, tenuto debito conto dello stato dell'arte,

a far sì che i titolari del trattamento e i responsabili del trattamento possano adempiere ai loro obblighi di protezione dei dati. I principi della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita dovrebbero essere presi in considerazione anche nell'ambito degli appalti pubblici."

Sia *data protection by design* che *data protection by default* sono molto importanti in termini di responsabilità giuridica del titolare del trattamento. Infatti l'articolo 24 del GDPR sancisce in capo al titolare l'onere di mettere in atto "misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento".[19]

3.5.8 L'attuazione dei principi Privacy

L'articolo 5, comma 1, lettera a) del GDPR stabilisce che i dati personali devono essere trattati in maniera lecita, corretta e trasparente. Inoltre il regolamento si basa sul principio della responsabilizzazione che pone in capo al titolare del trattamento dei dati personali l'obbligo di adottare misure tecniche e organizzative idonee a garantire il rispetto del diritto alla protezione dei dati e le libertà fondamentali dell'uomo. Tali misure vengono attuate in seguito ad appropriate valutazioni di impatto privacy qualora il trattamento presenta dei rischi che potrebbero compromettere i diritti e le libertà fondamentali dell'interessato. Al fine di garantire un trattamento dei dati lecito e corretto nel rispetto della disciplina sulla protezione dei dati il *Data Protection Officer (DPO)* o responsabile della protezione dati – nuova figura introdotta dal Regolamento europeo in materia di privacy – ha, tra i suoi compiti elencati all'articolo 39, l'incarico di *"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."*

Per quanto riguarda l'Italia, il Codice della privacy antecedente le modifiche apportate del D. Lgs. n. 101/2018 in tema di principi generali presenta similitudini con il Regolamento europeo, l'unica accortezza su cui viene posta l'attenzione da parte del Legislatore è quella di invitare l'interprete a cogliere la modalità di applicazione dei principi generali in materia di privacy.

3.6 I diritti dell'interessato

Il Capo III del Regolamento generale sulla protezione dei dati è dedicato ai diritti dell'interessato, alcuni di essi erano già presente nella normativa europea in materia di privacy, altri invece costituiscono una novità introdotta con il Regolamento. Per quanto

[19] Articolo 24, comma 1 del GDPR.

riguarda i diritti già previsti nella Direttiva 95/46/CE, questi subiscono una modifica sia nella struttura che nella modalità di esercizio.
La causa principale delle modifiche e delle novità apportate dal GDPR va individuata nel continuo progresso tecnologico, il quale grazie all'introduzione di nuovi strumenti nel campo della digitalizzazione e il loro sempre più vasto utilizzo hanno sottolineato la necessità di rafforzare il diritto alla privacy, o come meglio viene definito dal Regolamento, il diritto alla protezione dei dati, quale diritto fondamentale.

La normativa italiana in merito ai diritti dell'interessato – trattati al Titolo II del Codice della Privacy – è stata abrogata dal D. Lgs. 10 agosto 2018, n. 101, il quale rinvia al Regolamento europeo.

3.6.1 Il diritto all'informazione

La Sezione 1 del Capo III tratta le modalità di esercizio dei diritti insieme al diritto all'informazione, descrivendo gli obblighi in capo al titolare del trattamento, tra cui quello del rispetto del principio della trasparenza, già trattato precedentemente.

L'articolo 12 comma 1, infatti stabilisce 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"*. Di fondamentale importanza è la forma che il titolare del trattamento utilizza nell'informare l'interessato, questa deve essere *"concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro"*, di norma l'informazione all'interessato circa il trattamento dei suoi dati deve avvenire in forma scritta o con modalità elettroniche. È ammessa anche la forma orale se rispettate 2 condizioni: deve persistere una richiesta dell'interessato, e deve essere comprovata con altri mezzi l'identità dell'interessato.

Inoltre l'articolo 12 sancisce il termine entro il quale il titolare è tenuto a dare riscontro all'interessato, anche in caso di diniego. Tale termine è di un mese dal ricevimento della richiesta stessa, termine che può essere derogabile di due mesi in casi di particolare complessità. Spetta al titolare valutare il grado di complessità della richiesta. In caso di diniego, il titolare comunque è tenuto a dare riscontro all'interessato entro il termine prefissato motivando l'inottemperanza ed informandolo della *"possibilità di proporre recla-*

mo a un'autorità di controllo e di proporre ricorso giurisdizionale".[20] Sempre l'articolo 12 stabilisce che il riscontro all'interessato viene fornito a titolo gratuito. Qualora si è in presenza di richieste infondate o eccessive - il cui carattere infondato o eccessivo deve essere dimostrato dal titolare – il titolare può chiedere all'interessato un'eventuale contributo per il riscontro. (art. 12, comma 5).

Successivamente, agli articoli 13 e 14 vengono individuate rispettivamente le *"Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato"* e le *"Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato"*. Questi due articoli sono rimasti sostanzialmente tali quali gli articoli 10 e 11 della Direttiva 95/46/CE. Inoltre il diritto all'informazione ha origini ben più lontane, infatti esso veniva previsto già nell'articolo 8, lettera a) della Convenzione 108 risalente al 1981.

3.6.2 Il diritto di accesso

Il diritto di accesso viene trattato all'articolo 15, il quale prevede: *"L'interessato ha il diritto di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere l'accesso ai dati personali"* ed inoltre ad un serie di informazioni che vengono elencate al comma 1, tra cui le finalità del trattamento, i destinatari a cui i dati personali saranno comunicati, con particolare attenzioni se i destinatari sono di Paesi terzi (argomento che verrà trattato a parte al Capo V del presente Regolamento), il periodo di conservazione dei dati. Inoltre viene menzionato il diritto dell'interessato di *"chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento; il diritto di proporre reclamo a un'autorità di controllo".*[21]

Anche il diritto di accesso persisteva nella Direttiva "madre" e veniva trattato all'articolo 12 lett. a), inoltre era previsto anche all'articolo 8 lett. b) della Convenzione 108. A differenza dei precedenti strumenti giuridici in materia di privacy, il Regolamento UE n. 2016/679 tende a disciplinare la materia in modo più preciso e minuzioso.

3.6.3 Il diritto di rettifica

L'articolo 16 sancisce che: *"L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa."*

[20] Articolo 12, comma 4 – GDPR.
[21] Articolo 15, comma 1, lett. e) ed f) – GDPR.

3.6.4 Il diritto all'oblio

Il diritto all'oblio o il diritto alla cancellazione dei dati lo si individua anche all'articolo 12, lettera b) della Direttiva 95/46/CE, il quale prevede il diritto dell'interessato di ottenere dal titolare la "la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati". Inoltre questo diritto era presente anche nella Convenzione 108 all'articolo 8, lettera c).

La novità introdotta dal Regolamento generale sulla protezione dei dati consiste nell'articolazione e nella particolarizzazione di tale diritto. Il diritto alla cancellazione dei dati è recepito dall'articolo 17, che obbliga i titolari a provvedere alla cancellazione dei dati dell'interessato senza indebito ritardo qualora sussistano tutta un serie di situazioni, le quali:

a) *"i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati;*

b) *l'interessato revoca il consenso su cui si basa il trattamento [...];*

c) *l'interessato si oppone al trattamento ai sensi dell'articolo 21;*

d) *i dati personali sono stati trattati illecitamente;*

e) *i dati personali devono essere cancellati per adempiere un obbligo giuridico 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."*

Ma la novità più sostanziale va individuato al secondo paragrafo, ovvero l'obbligo in capo al titolare del trattamento di informare della richiesta di cancellazione altri titolari che trattano i dati cancellati, compresi *"qualsiasi link, copia o riproduzione dei suoi dati personali."*[22]

Rispetto al Codice della Privacy, l'articolo 17 del Regolamento europeo è più ampio grazie alle novità introdotte. Ad esempio un'altra novità è il riconoscimento del diritto dell'interessato di chiedere la cancellazione dei propri dati anche in seguito alla revoca del consenso al trattamento. Infine, il paragrafo 3 prevede tutta una serie di casi in cui il diritto all'oblio non può essere esercitato.

L'articolo 17 accoglie in parte la giurisprudenza della Corte di Giustizia dell'UE espressa durante la sentenza del 13 maggio 2014 riguardante il famoso caso, precedentemente citato,

[22] Articolo 17, paragrafo 2 – GDPR, Capo III – I diritti dell'interessato.

Google Spain SL e Google Inc. contro Agencia Española de Protección de Datos (AEPD) e Mario Costeja González.[23]

3.6.5 Il diritto alla portabilità dei dati

Il diritto alla portabilità dei dati è una novità assoluta introdotta dal Regolamento UE n. 2016/679 all'articolo 20. Data la sua importanza si riporta di seguito il testo del citato articolo:

1. *"L'interessato ha il diritto 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 e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti qualora:*

   a) *il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b); e*

   b) *il trattamento sia effettuato con mezzi automatizzati.*

2. *Nell'esercitare i propri diritti relativamente alla portabilità dei dati a norma del paragrafo 1, l'interessato ha il diritto di ottenere la trasmissione diretta dei dati personali da un titolare del trattamento all'altro, se tecnicamente fattibile.*

3. *L'esercizio del diritto di cui al paragrafo 1 del presente articolo lascia impregiudicato l'articolo 17. Tale diritto non si applica al trattamento 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.*

4. *Il diritto di cui al paragrafo 1 non deve ledere i diritti e le libertà altrui."*

Innanzitutto viene sottolineato l'ambito di applicazione del presente diritto, che si applica solo ai trattamenti automatizzati. Inoltre, l'Autorità Garante nazionale nelle Linee guida interpretative definisce quali sono i dati portabili: *"sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato"*, come definito anche dalla stesso articolo 20 del GDPR al paragrafo 1.

In primis, tale articolo sancisce il diritto dell'interessato di ricevere i propri dati dal titolare del trattamento per poterli conservare privatamente al fine di riutilizzarli in futuro se ritenuto necessario. Per permettere all'interessato la gestione e il riutilizzo dei propri dati il titolare deve adottare *"un formato strutturato, di uso comune e leggibile da dispositivo*

[23] Caso cit. Supra note 10.

automatico" dei dati trattati. Per questa ragione il diritto alla portabilità dei dati costituisce un'integrazione del diritto di accesso sancito all'articolo 15 del Regolamento europeo. Inoltre, secondo il Parere del Gruppo di Lavoro (WP 29) in merito alla portabilità dei dati *"I Titolari del trattamento devono informare gli interessati sulla disponibilità del diritto di portabilità (ad esempio prima della chiusura di un account) e sono incoraggiati a garantire l'interoperabilità del formato dei dati forniti a fronte di una richiesta di portabilità. Questo ultimo aspetto riveste particolare rilevanza per il mondo IT, che sarà chiamato a rendere praticabili questi adempimenti."*[24]

In secondo luogo, l'articolo 20 sancisce il diritto dell'interessato di trasmettere i dati da un titolare all'altro senza ostacoli.

Dunque l'articolo 20 è un'innovazione in tema di diritti dell'interessato, in quanto esso prevede una facilitazione della capacità degli interessati di trasmettere e gestire i dati che lo riguardano e nello stesso tempo, una promozione dell'innovazione e della condivisione dei dati personali tra vari titolari del trattamento in modo protetto e sicuro e sotto il vigile controllo dell'interessato. Il diritto alla portabilità dei dati è una disposizione intenta a garantire agli interessati il maggior controllo sui propri dati personali. A tal proposito il considerando 68:

"Per 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. È opportuno incoraggiare i titolari del trattamento a sviluppare formati interoperabili che consentano la portabilità dei dati[...]"

3.6.6 Il diritto di opposizione

L'articolo 21 riconosce all'interessato *"il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f), compresa la profilazione*[25] *sulla base di tali disposizioni."* Qualora l'interessato abbia esercitato tale diritto, il titolare deve astenersi dal trattare ulteriormente i dati, o dimostrare l'esistenza di motivi legitti-

[24] P. CALVI, *Portabilità: Linee guida del WP 29* , in "Europrivacy", 24 dicembre 2016

[25] La "profilazione" viene definita all'articolo 4 del nuovo Regolamento 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; (C24, C30, C71-C72)".

mi per i quali i dati devono continuare ad essere trattati. Tali motivi si ritengono validi qualora prevalgano *"sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria."*

Inoltre al paragrafo 2 viene menzionata la facoltà di opporsi in capo all'interessato anche qualora i dati siano trattati per finalità di marketing diretto in qualsiasi momento. Se egli esercita il diritto di opporsi al trattamento per finalità di marketing diretto, in base al paragrafo successivo *"i dati personali non sono più oggetto di trattamento per tali finalità."*

Anche nel caso i dati personali vengano trattati a fini di ricerca scientifica o a fini storici o statistici viene riconosciuto all'interessato il diritto di opporsi. L'unica eccezione viene fatta nel caso in cui il trattamento serve nel eseguire un compito di pubblico interesse.[26] Ad ogni modo il Regolamento prevede all'articolo 89 delle garanzie e delle deroghe specifiche con le quale intende conciliare le necessità della ricerca scientifica, storica o statistica con i diritti dell'interessato.

3.6.7 Le limitazioni

L'articolo 23 – ultimo del Capo III – prevede delle limitazioni dei diritti e degli obblighi sanciti agli articoli da 12 a 22 e 34 e qualvolta all'articolo 5, tramite misure legislative. Tenuto conto dei diritti e delle libertà fondamentali dell'uomo, come sottolineato dal considerando 73,[27] queste limitazioni vengono fatte in quanto ritenute necessarie in una società democratica, al fine di proteggere la sicurezza nazionale, la sicurezza pubblica, la difesa, la prevenzione, l'indagine, il perseguimento di reati, l'esecuzione di sanzioni penali, la tutela dell'interessato o dei diritti e delle libertà altrui, ecc.[28]

Questo articolo ha come predecessore l'articolo 13 della Direttiva 95/46/CE.

3.7 Titolare e responsabile del trattamento

Se da un lato il Legislatore europeo ha provveduto al riconoscimento dei diritti dell'interessato, dall'altro esso ha dedicato parte del Regolamento anche agli obblighi in capo al titolare e al responsabile del trattamento. Non a caso il Capo successivo del Regolamento UE n. 2016/679 viene dedicato per intero alla figura del titolare del trattamento e a quella del responsabile del trattamento.

[26] Articolo 21, paragrafo 6 – GDPR.
[27] Considerando 73, GDPR: "[...]. Tali limitazioni dovrebbero essere conformi alla Carta e alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali."
[28] Articolo 23, paragrafo 1 – GDPR.

3.7.1 Il titolare del trattamento

Innanzitutto per titolare del trattamento si intende: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri"*.[29]

Il titolare del trattamento copre la funzione di vertice che:

a. provvede al rispetto dei principi generali dettati dal presente regolamento all'articolo 5, paragrafo 2, in quanto in base al principio dell'*accountability* è ritenuto responsabile qualora i principi non venissero applicati al trattamento dei dati personali;

b. realizza un sistema di gestione privacy con l'adozione di misure tecniche e organizzative adeguate al fine di garantire e dimostrare che il trattamento viene effettuato in modo conforme al Regolamento;

c. si occupa della sicurezza del trattamento (art. 32), applicando i principi di *privacy by design* e *privacy by default* (art. 25);

d. effettua un'accurata valutazione d'impatto privacy dei trattamenti (art. 35);

e. adotta *policy* sul trattamento dei dati personali (art. 24, paragrafo 2) o aderisce a codici di condotta (art. 40) o consegue certificazioni (art. 42);

f. in base agli articoli 13 e 14, rende idonea l'informativa agli interessati;

g. fornisce riscontro alle richieste dell'interessato, qualora egli intenda esercitare i suoi diritti (art. 12, paragrafo 3 e artt. 15-22);

h. si dedica alla notifica di violazione dei dati personali (*data breach notification*) – qualora esistono le condizioni – la quale verrà comunicata all'Autorità Garante e all'interessato entro 72 ore previste dal Regolamento (artt. 33 e 34);

i. coopera con l'Autorità Garante (art. 31), alla quale fornisce ogni informazione ritenuta esigente;

j. nomina i responsabili del trattamento, come sanciscono gli articoli 24, paragrafo 1 e 28 paragrafo 1;

k. nomina il Responsabile Protezione Dati (o *Data Protection Officer – DPO*) ai sensi dell'articolo 37, paragrafo 5, con il quale coopera (art. 38, paragrafo 1), lo sostiene

[29] Definizione fornita dallo stesso Regolamento europeo all'articolo 4, paragrafo 1, n. 7).

nello svolgimento dei suoi compiti (art. 38, paragrafo 2), assicurandogli indipendenza e autonomia (art. 38, paragrafo 3).[30]

Dunque come si evince la figura del titolare gioco un ruolo fondamentale al interno del trattamento dei dati personali e tale importanza gli conferisce il potere decisionale.

Un altro punto di notevole importanza è dato dal fatto che il Regolamento generale sulla protezione dei dati prevede la contitolarità, la quale viene disciplinata all'articolo 26. Ai titolari del regolamento è imposto di definire il rispettivo ambito di responsabilità e i vari compiti di ciascuno di essi, tenendo conto in modo particolare dell'esercizio dei diritti dell'interessato, quest'ultimo può comunque *"esercitare i propri diritti nei confronti di e contro ciascun titolare del trattamento"*.[31] Tale definizione deve avvenire tramite un atto giuridico valido in base al diritto nazionale. Questo accordo, ai sensi dell'art. 26, paragrafo 1, *"può designare un punto di contatto per gli interessati."*

Per quel che riguarda le caratteristiche soggettive e le responsabilità del titolare del trattamento descritte dal Regolamento UE n. 2016/679, esse erano già state definite all'interno della Direttiva "madre". L'unica eccezione è il già citato principio di responsabilizzazione, il quale veniva definito dalla Direttiva 95/46/CE. Infatti, il principio dell'*accountability* viene introdotto successivamente dal Gruppo di lavoro Articolo 29 (WP 173) nel parere n. 3/2010 "sul principio di responsabilizzazione".[32]

Il Regolamento ribadisce all'articolo 24 la responsabilità in capo al titolare del trattamento, il quale ha il dovere di attuare misure tecniche e organizzative idonee al fine di garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al RGPD.

3.7.2 Il responsabile del trattamento

L'articolo 4, n. 8 definisce il responsabile del trattamento come: *"la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento."*

Il responsabile del trattamento è un soggetto esterno, non un dipendente del titolare del trattamento. Infatti nella sua figura viene individuato un fornitore al quale è esternalizzato un determinato trattamento.

[30] Op. cit. Supra note 8, pp. 107-108.
[31] Articolo 26, paragrafo 3 – GDPR.
[32] Gruppo di Lavoro Articolo 29, parere n. 3/2010 "sul principio di responsabilizzazione", testo integrale consultabile online sul sito ufficiale del Garante Privacy.

Sostanzialmente il Regolamento presenta parti comuni con la Direttiva 95/46/CE. La parte che si differenzia dalla disposizione precedente in materia di protezione dei dati si riferisce all'atto di nomina del responsabile del trattamento – trattata all'articolo 28, paragrafo 3 – che presenta contenuti più dettagliati rispetto alla Direttiva "madre".

Infatti, l'atto di nomina, come viene definito all'articolo 28, paragrafo 3:

"I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento." Inoltre il paragrafo 3 dell'articolo 28 prevede tutta una serie di funzioni che deve svolgere il responsabile del trattamento, tra queste quella di garantire *"[...] che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza".*[33] Inoltre gli viene richiesto di assistere il titolare nell'attuazione di misure tecniche e organizzative idonee per adempiere alle richieste dell'esercizio dei diritti degli interessati (art. 28, paragrafo 3, lettera e)). La sua assistenza al titolare è richiesta anche al fine di garantire l'adempimento agli obblighi previsti dagli artt. 32-36 (art. 28, paragrafo 3, lettera f)). Il responsabile deve mettere a disposizione del titolare tutte le informazioni utili per dimostrare il rispetto degli obblighi dettati da questo articolo, ed inoltre consente e contribuisce alle attività di revisione effettuate dal titolare stesso o da un altro soggetto da lui incaricato (art. 28, paragrafo 3, lettera h)). Oltre a questi obblighi in capo al responsabili previsti all'articolo 28, il Regolamento aggiunge anche ulteriori adempimenti, tra cui:

- assistere il titolare, nella valutazione d'impatto privacy (*Data Protection Impact Assessment*) o di preventiva consultazione con l'Autorità Garante (a tal riguardo si veda il considerando 95);

- collaborare con l'Autorità Garante ai sensi degli artt. 31 e 58;

- cooperare con gli Organismi indipendenti di certificazione in base all'art. 42, paragrafo 6);

- sostenere il Responsabile della Protezione dei Dati nello svolgimento della sua attività con ogni mezzo, informazione a accessi a sua disposizione (art.38, paragrafo 2).[34]

[33] Articolo 28, paragrafo 3, lettera b) – GDPR.
[34] Op. cit. Supra note 8, p. 116.

3.7.3 I registri delle attività di trattamento

La tenuta dei registri delle attività del trattamento rientra tra gli obblighi in capo sia al titolare del trattamento sia al responsabile del trattamento. Tale obbligo viene previsto all'articolo 30 paragrafo 1 e 2. Il registro delle attività di trattamento contiene informazioni, quali:

- il nome e i dati di contatto del titolare, del responsabile, e ove previsto del contitolare nel caso di registro del titolare, del rappresentate sia del titolare che del responsabile e dove previsto anche i dati del DPO;
- le finalità del trattamento;
- categorie di interessati e categorie di dati personali trattati;
- i destinatari a cui i dati trattati saranno comunicati, inclusi i destinatari di paesi terzi od organizzazioni internazionali;
- la documentazione riguardante le garanzie adeguate, qualora i dati vengano trasferiti verso un paese terzo od un'organizzazione internazionale, nonché l'individuazione del paese terzo o dell'organizzazione internazionale;
- una descrizione generale delle misure di sicurezza tecniche e organizzativi previste all'articolo 32, paragrafo 1.[35]

Sempre l'articolo 30 stabilisce al paragrafo 3 che i registri delle attività di trattamento devono essere tenuti in forma scritta, ed è ammessa la loro tenuta anche in formato elettronico.

Inoltre, tale registro deve essere messo a disposizione dell'Autorità Garante, se espressamente richiesto. (art. 30, paragrafo 4).

Infine al paragrafo 5 viene definito l'ambito di applicazione dell'obbligo di tenere il registro delle attività di trattamento. Infatti, non tutti i titolari e i responsabili del trattamento devono adempiere a tale disposizione. Questa norma viene applicata soltanto alle imprese od organizzazioni con più di 250 dipendenti, a meno che non vi sia presente un rischio che comprometterebbe i diritti e le libertà fondamentali dell'interessato, o *"il trattamento non sia occasionale o includa il trattamento di categorie particolari di dati di cui all'articolo 9, paragrafo 1, o i dati personali relativi a condanne penali e a reati di cui all'articolo 10."*[36]

In merito, alla tenuta dei registri delle attività di trattamento, il considerando 82:

[35] Articolo 30, paragrafo 1 e 2 – GDPR.
[36] Articolo 30, paragrafo 5 – GDPR.

"Per dimostrare che si conforma al presente regolamento, il titolare del trattamento o il responsabile del trattamento dovrebbe tenere un registro delle attività di trattamento effettuate sotto la sua responsabilità. Sarebbe necessario obbligare tutti i titolari del trattamento e i responsabili del trattamento a cooperare con l'autorità di controllo e a mettere, su richiesta, detti registri a sua disposizione affinché possano servire per controllare detti trattamenti."

3.8 Il Responsabile della Protezione dei dati

Il Responsabile della Protezione dei Dati (RPD) o *Data Protection Officer (DPO)* è la nuova figura soggettiva introdotta dal Regolamento UE n. 2016/679 con la finalità di sostenere il titolare e il responsabile del trattamento nell'attuazione di tutte le misure tecniche e organizzative nell'ottica dell'*accountability*, su cui si basa l'intero Regolamento. Il RGPD dedica 3 articoli: 37, 38 e 39 alla figura del *Data Protection Officer*, considerata dallo stesso Regolamento uno degli elementi-chiave all'interno del nuovo sistema di *governance* dei dati.[37]

Si tiene a precisare il fatto che tale figura sostiene il titolare e il responsabile del trattamento, ma non mette in atto le misure tecniche e organizzative idonee per garantire che il trattamento venga fatto in conformità al GDPR. Dunque il rispetto delle disposizioni previste dal Regolamento europea è sotto la responsabilità del titolare del trattamento e non del DPO. Infatti, in tutti gli articoli fin ora esaminati si nominano le figure del titolare e del responsabile del trattamento nell'attuare le misure adeguate, nel tenere un registro delle attività di trattamento, ecc. Ovviamente il fatto che la figura del DPO non venga citata all'esecuzione degli obblighi in capo al titolare, non esclude il fatto che egli non possa comunque adempiere a tali obblighi su richiesta del titolare, come ad esempio la tenuta del registro, come veniva sottolineato dal WP29 nel Parere del 13 dicembre 2016.[38]

3.8.1 La nomina del Responsabile della Protezione dei Dati

Il primo articolo che viene dedicato alla nuova figura del DPO, l'articolo 37, tratta l'atto di nomina del Responsabile della Protezione dei Dati. L'articolo 37 non distingue se il titolare o il responsabile debba nominare il DPO, ma fornisce un elenco di casi in cui la nomina del Responsabile della Protezione dei dati è obbligatoria, i quali:

a) *"il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;*

[37] Op. cit. Supra note 8, p. 125.
[38] Ibidem.

b) *le attività principali del titolare del trattamento o del responsabile del trattamento*[39] *consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;*[40] *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 o di dati relativi a condanne penali e a reati di cui all'articolo 10."*[41]

Questo non esclude la nomina facoltativa. Per i titolari e i responsabili del trattamento qualora decidessero volontariamente di nominare un Responsabile della Protezione dei Dati, essi sono tenuti a rispettare le disposizioni di cui agli artt. 37, 38 e 39 come nel caso della nomina obbligatoria.[42]

Al paragrafo successivo viene stabilito che un gruppo imprenditoriale può nominare un unico DPO solo se egli è facilmente raggiungibile da ciascun stabilimento.

In seguito, ai sensi del paragrafo 3 un unico Responsabile della Protezione dei Dati può essere designato per più autorità pubbliche o organismi pubblici, tenuto conto della loro dimensione e struttura organizzativa.

Di fondamentale importanza è il paragrafo 5, secondo il quale: *"Il responsabile della protezione dei dati è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica*[43] *della normativa e delle prassi in materia di protezione dei dati,*

[39]"Le attività principali di un titolare del trattamento riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria." (Considerando 97, GDPR).

[40]L'espressione "trattamento su larga scala" non viene esplicitamente definita dal Regolamento, ma il considerando 91 relativo alla valutazione d'impatto privacy definisce: "i trattamenti su larga scala ai trattamenti su larga scala, 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, ad esempio, data la loro sensibilità, laddove, in conformità con il grado di conoscenze tecnologiche raggiunto, si utilizzi una nuova tecnologia su larga scala, nonché ad altri trattamenti che presentano un rischio elevato per i diritti e le libertà degli interessati, specialmente qualora tali trattamenti rendano più difficoltoso, per gli interessati, l'esercizio dei propri diritti". Ad esempio possono essere considerati trattamenti su larga scala i trattamenti di dati riguardanti i pazienti di un ospedale, trattamenti di dati che riguardano i clienti da parte di una banca o di un'impresa assicurativa oppure i trattamenti di dati degli utenti da parte di un motore di ricerca a fini di pubblicità comportamentale.

[41]Articolo 37, paragrafo 1 – GDPR

[42]WP 243, p. 5.

[43]Le qualità professionali e la conoscenza specialistica non trovano definizione all'interno del Regolamento. Per qualità professionali sicuramente si fa riferimento al fatto che RPD deve avere un'ottima conoscenza delle disposizioni dettate dal presente regolamento e di quelle nazionali, nonché deve conoscere la prassi sia nazionale che europea in merito alla protezione dei dati. Mentre per conoscenza specialistica si intende che il DPO deve possedere il più alto livello di conoscenze in base alla caratteristiche dei trattamenti di dati personali.

e della capacità di assolvere i compiti di cui all'articolo 39."[44]

Qualora si decidesse di nominare un DPO esterno, il rapporto che si instaura tra il titolare del trattamento (o il responsabile del trattamento) e il *Data Protection Officer* si basa su un contratto di servizi, il che esclude il fatto che il DPO sia un dipendente del titolare del trattamento (art. 37, paragrafo 6).

Infine la disposizione prevede l'obbligo in capo al titolare e al responsabile del trattamento di comunicare i dati del DPO designato all'Autorità di controllo, in quanto tra i compiti del DPO vi è quello di cooperare con l'Autorità di controllo (art. 39, paragrafo 1, lett. d)).

3.8.2 La posizione del Responsabile della Protezione dei Dati

Per quanto riguarda la posizione del DPO, in base all'articolo 38, paragrafo 1 *"Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali."*[45] Il fatto che venga prevista la tempestività del coinvolgimento della figura del DPO in ogni questione riguardante la protezione dei dati evidenzia l'importanza della funzione che egli svolge all'interno del sistema di *governance* dei dati. Inoltre, facendo riferimento alla valutazione d'impatto privacy, il suo coinvolgimento immediato è previsto dal RGPD, affinché il DPO possa contribuire a tale valutazione fin dalla fase iniziale, ovvero la fase di progettazione di un trattamento dei dati personali (art.35, paragrafo 1). Oltre al Regolamento, un'altra fonte che ha espresso il suo parere in merito, il Gruppo di Lavoro (WP29), infatti il WP29 sottolinea l'importanza del coinvolgimento immediato del DPO, attraverso la sua consultazione ed informazione fin dalla fase di progettazione, renderà più facile il rispetto della normativa europea in materia di protezione dei dati (RGPD), l'applicazione dei principi privacy fin dalla progettazione del trattamento dei dati personali. Al fine di verificare se la figura del DPO è stata coinvolta fin da subito in ogni questione attinente alla protezione dei dati, il WP29 presenta un elenco di indicatori, tra i quali: il RPD partecipa alle riunioni del management, è presente ogni volta che vengono prese decisioni che apporteranno un impatto sulla protezione dei dati; gli vengono date tutte le informazioni a disposizione riguardante i trattamenti per avere una consulenza adeguata in merito, i suoi consigli vengono presi in considerazione dal management ed infine, qualora si verifichi un *data breach*, egli viene consultato immediatamente.[46]

[44] Articolo 37, paragrafo 5 – GDPR.
[45] Articolo 38, paragrafo 1 – GDPR.
[46] Op. cit. Supra note 8, p. 135.

Proseguendo sulle disposizioni dell'articolo 38, al paragrafo 2 si chiede al titolare del trattamento e al responsabile del trattamento di mettere a disposizione del DPO tutte le risorse necessarie per poter adempiere ai suoi compiti previsti all'articolo 39. Persiste una relazione diretta tra il livello di complessità e/o di sensibilità e le risorse necessarie: all'aumentare del livello di complessità e/o di sensibilità dei dati trattati aumentano anche le risorse necessarie per assolvere i compiti.

Il Regolamento inoltre prevede al paragrafo 3 dell'articolo 38 che il Responsabile della Protezione dei Dati sia indipendente, e per garantirle tale autonomia nell'eseguire i suoi compiti, viene chiesto al titolare e al responsabile del trattamento di non dare alcuno istruzione al DPO su come egli debba adempiere ai suoi doveri.

Inoltre, ai sensi dell'articolo 38, paragrafo 3 viene stabilito che: *"Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento."*[47] Tale situazione si verifica allorquando il titolare o il responsabile del trattamento non tengono conto dei consigli del DPO e prendono decisioni non conformi con il Regolamento. In merito, il DPO ha la possibilità di comunicare il suo disaccordo al management di alto livello. Questo rapporto diretto con il vertice amministrativo fa sì che quest'ultimo sia informato riguardo alla consultazione fornita dal DPO al titolare o responsabile del trattamento, soggetti su cui si riversa la responsabilità dell'ottemperanza della disposizione in materia della protezione dei dati ed inoltre, devono dimostrare di aver rispettato tale normativa.[48]

Successivamente, al paragrafo 4 viene definito il rapporto tra il DPO e gli interessati, questi ultimi possono rivolgersi al Responsabile della Protezione dei Dati per tutte le situazioni riferite al trattamento dei loro dati personali e all'esercizio dei loro diritti di cui al Capo III del GDPR.

Sempre in capo al DPO vi è l'obbligo alla riservatezza riguardante l'esecuzione dei suoi compiti conformemente al diritto europeo e degli Stati membri (art. 38, paragrafo 5).

Oltre ai compiti a cui deve adempiere ai sensi dell'articolo 39, il DPO può eseguire anche altri compiti e coprire anche altre funzioni, rispettando però un'unica condizione, ovvero quella di avere la garanzia da parte del titolare o responsabile del trattamento dell'assenza

[47] Articolo 38, paragrafo 3 – GDPR.
[48] Op. cit. Supra note 8, pp. 136-137.

del conflitto di interessi tra le varie mansioni e funzioni svolte dalla figura del DPO (art. 38, paragrafo 6).

3.8.3 I compiti del Responsabile della Protezione dei Dati

I compiti del Responsabile della Protezione dei Dati invece vengono elencati all'articolo 39, paragrafo 1 del Regolamento generale sulla protezione dei dati. Questi sono i seguenti:

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;*

d) *cooperare con l'autorità di controllo; e*

e) *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."*[49]

Oltre a questi compiti, il considerando 97 aggiunge in merito: *"il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento."*

Si tiene a precisare ulteriormente che il fatto che il DPO assista il titolare o il responsabile del trattamento nel verificare il rispetto delle disposizioni previste dal GDPR all'interno dell'organizzazione aziendale non implica che egli ne sia personalmente responsabile in caso di inottemperanza.

In termini di valutazione d'impatto sulla protezione dei dati[50] il DPO non ha l'obbligo di effettuare tale valutazione, mentre tale obbligo è in capo al titolare del trattamento dei

[49] Articolo 39, paragrafo 1 – GDPR.
[50] In Inglese Data Protection Impact Assessment – acronimo DPIA.

dati ai sensi dell'articolo 35, paragrafo 1. Il Responsabile della Protezione dei Dati invece contribuisce alla DPIA con il suo parere qualora richiesto dal titolare (art. 39, paragrafo 1, lett. c)). Tuttavia, considerato il suo ruolo-chiave all'interno del trattamento, la sua assistenza al titolare nell'effettuare la valutazione d'impatto sulla protezione dei dati risulta di notevole importanza ed efficacia. Ecco che in osservanza del principio di protezione dei dati fin dalla fase di progettazione (Data Protection by Design), il Regolamento contempla all'art. 35, paragrafo 2 che il titolare nell'elaborazione di una DPIA si consulta con il DPO.

Per quel che riguarda invece, le lettere d) ed e), ovvero il compito di cooperare con l'Autorità di controllo e quello di essere il punto di contatto per l'Autorità di controllo. Tali doveri in capo al DPO hanno il fine di facilitare l'accesso, da parte dell'Autorità di controllo, alle informazioni e ai documenti necessari per lo svolgimento dei compiti previsti all'articolo 57 e l'esercizio dei poteri stabiliti all'articolo 58.

In base all'articolo 39, paragrafo 2 si evince che il DPO nell'adempiere ai suoi compiti segue l'approccio fondato sul rischio, ovvero il DPO si occupa in via prioritaria delle questioni con rischi più alti.

3.9 Il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali

Il Regolamento UE n. 2016/679 tratta il trasferimento di dati personali verso Paesi terzi o organizzazioni internazionali al Capo V, agli articoli da 44 a 50. Il trasferimento dei dati verso Paesi extra-europei non costituisce una novità introdotta dal regolamento. Tale tema è stato affrontato per la prima volta dalla Convenzione europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali del 1950 con la conferma del concetto di privacy come diritto fondamentale dell'uomo a livello transnazionale. La CEDU non è stata l'unica disposizione in tema di privacy, soprattutto con riguardo al flusso di dati transfrontalieri. In merito, le Linee guida dell'Organizzazione per la cooperazione e lo sviluppo economico (OCSE) trent'anni più tardi ha sviluppato il primo esempio pratico introducendo alcuni principi base della protezione dei dati a livello internazionale. Uno di questi principi stabilisce una limitazione del trasferimento dei dati sensibili verso Paesi terzi, qualora la tutela dello Stato mittente sia maggiore di quella dello Stato ricevente, cioè non equivalente. La connotazione di equivalenza viene riconsiderata dalla Convenzione n.108, in base alla quale se non viene rispettato questo principio (principio di protezione equivalente) è possibile l'interruzione del trasferimento dei dati personali. Quattro anni più tardi, il 14 giugno del 1985 vengono firmati gli Accordi di Shenghen, i quali, richiamando la Convenzione di Strasburgo, riconfermano l'equivalenza della protezione dei dati in questi termini:*"ciascuna Parte adotterà [...] le disposizioni nazionali necessarie per ottenere un*

livello di protezione dei dati personali almeno pari a quello derivante dai principi della Convenzione del Consigli d'Europa del 28 gennaio 1981 sulla protezione delle persone nei riguardi del trattamento automatizzato dei dati di natura personale" (art. 126, Convenzione 14 giugno 1985, Accordi di Shenghen).[51]

Ma il punto di svolta in tema di trasferimento di dati verso l'esterno si ha con l'entrata in vigore del Trattato di Maastricht (1 novembre 1993). Come già trattato nel capitolo 2 del presente elaborato, il Trattato di Maastricht introduce all'art. 7 lo sviluppo del mercato interno, il quale necessità anche il bisogno di garantire la circolazione dei dati personali da uno Stato membro all'altro, inoltre ci deve essere un tutela dei diritti equivalente nei diversi Paesi UE. In risposta a queste esigenze nasce la Direttiva 95/46/CE che intende perseguire entrambi gli obbiettivi. Per garantire la tutela della privacy, oltre agli strumenti giuridici a disposizione, un ruolo complementare e di fondamentale importanza viene attribuito dalla Commissione europea all'impiego di misure tecnologiche. E il Regolamento UE n. 2016/679, sulla scia della Direttiva "madre", riconferma tale affermazione e facendo una considerazione sul progresso tecnologico e sulle conseguenze che esso apporta in merito alla circolazione dei dati.

"La rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali. La portata della condivisione e della raccolta di dati personali è aumentata in modo significativo. La tecnologia attuale consente tanto alle imprese private quanto alle Autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano. La tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso Paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali."[52]

3.9.1 Il trasferimento dei dati verso Paesi terzi nel Regolamento UE n. 2016/679

Il Regolamento dedica 8 articoli alla circolazione dei dati personali transfrontaliera, come accennato nel precedente paragrafo, l'intero Capo V si occupa di questa materia. In linea generale, le disposizioni previste dalla Direttiva 95/46/CE al Capo IV restano in vigore, con l'unica differenza che nel Regolamento scompare il requisito di autorizzazione nazionale di cui all'art. 44 del Vecchio Codice della Privacy.[53] Questo significa che il trasferimento di dati verso Paesi terzi può iniziare senza stare in attesa dell'autorizzazione

[51] Op. cit. Supra note 8, pp. 191-193.
[52] Ibidem.
[53] D. Lgs. n. 196/2003.

nazionale da parte del Autorità nazionale, a condizione che tale trasferimento sia "adeguato" ai sensi della decisione di adeguatezza della Commissione europea o in base alle norme vincolanti d'impresa,[54] o alle clausole contrattuali modello che fungono da garanzia di adeguatezza.
Tuttavia, qualora il trasferimento non si basi su una delle garanzie di adeguatezza di cui sopra ma su clausole contrattuali ad hoc predisposte dal titolare del trattamento resta necessaria l'autorizzazione da parte del Garante.

Ancor prima di fare un'analisi esaustiva in merito al trasferimento dei dati verso Paesi terzi o organizzazioni internazionali bisogna definire il concetto di "trasferimento", data la spontanea la domanda su cosa intende il Legislatore europeo per "trasferimento", dal momento che tale termine non trova definizione né all'interno della Direttiva "madre" né nel GDPR. Tale interrogativo fu posto dinnanzi alla Corte di giustizia dell'UE dalla Signora Lindqvist. Il caso riguardava la pubblicazione di dati personali su un sito web accessibile a tutti, anche a persone che si trovano in un Paese terzo. La problematica consisteva nel fatto che non si riusciva a definire se l'inserimento dei dati personali in un sito web costituisse o meno un trasferimento di dati. A tal riguardo la Corte di giustizia con sentenza del 6 novembre 2003 delibera che: *"non si configura un trasferimento verso un Paese terzo di dati ai sensi dell'articolo 25 della Direttiva 95/46 allorché una persona che si trova in uno Stato membro inserisce in una pagina Internet – caricata presso il suo fornitore di servizi di ospitalità (web hosting provider), stabilito nello Stato stesso o in un altro Stato membro – dati personali, rendendoli così accessibili a chiunque si colleghi ad Internet, compresi coloro che si trovano in Paesi terzi."*[55]

Una volta definita la connotazione di "trasferimento", si riprende il Regolamento generale sulla protezione dei dati e le disposizione dallo stesso previste in merito al tema trattato. In linea di principio il Regolamento vieta il trasferimento dei dati in una Stato terzo se quest'ultimo non assicura un livello di protezione dei dati personali adeguato. Tale adeguatezza viene verificata dalla Commissione europea mediante una decisione prevista all'articolo 25, paragrafo 6, della Direttiva 95/46/CE, normativa che non viene abrogata e continua ad essere applicata anche dallo stesso Regolamento (art. 45, paragrafo 9). Tuttavia se esistono delle specifiche garanzie, il trasferimento dei dati verso Paesi terzi è consentito. Il Regolamento fornisce un elenco predisposto in ordine gerarchico di tali

[54] Acronimo inglese BCR – Binding Corporate Rules. Le BCR sono definite dal Garante Privacy come: *"Si tratta di uno strumento volto a consentire il trasferimento di dati personali dal territorio dello Stato verso Paesi terzi (extra-UE) tra società facenti parti dello stesso gruppo dimpresa. Si concretizzano in un documento contenente una serie di clausole (rules) che fissano i principi vincolanti (binding) al cui rispetto sono tenute tutte le società appartenenti ad uno stesso gruppo (corporate). Le BCR costituiscono un meccanismo in grado di semplificare gli oneri amministrativi a carico delle società di carattere multinazionale con riferimento ai flussi intra-gruppo di dati personali."*

[55] Op. cit. Supra note 8, cit. p. 197.

garanzie:

a) adeguatezza del Paese terzo riconosciuta mediante decisione della Commissione europea;

b) in assenza di tale decisione di adeguatezza, spetta ai titolari coinvolti offrire garanzie adeguate previste da un contratto o pattuite, tra queste: le norme vincolanti d'impresa e le clausole contrattuali modello;

c) in assenza dei presupposti di cui sopra, è previsto l'utilizzo di deroghe al divieto di trasferimento applicabili in specifiche situazioni.

3.9.2 Trasferimento dei dati verso Paesi terzi sulla base della decisione di adeguatezza

La connotazione di adeguatezza viene introdotta dal Regolamento UE n. 2016/679 all'articolo 45, paragrafo 1, il quale conferma che: *"Il trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale è ammesso se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato. In tal caso il trasferimento non necessita di autorizzazioni specifiche."*

Ai sensi dell'articolo 45, paragrafo 8, la Commissione pubblica nella Gazzetta Ufficiale dell'UE e sul sito web l'elenco dei Paesi terzi e tutte quelle organizzazioni internazionali o imprese stabilite sul territorio di un Paese terzo, che non garantiscono più un livello di adeguatezza adeguato sulla base della decisione di adeguatezza da parte della Commissione stessa. Tali decisioni di adeguatezza hanno riguardato principalmente i seguenti Paesi: Andorra, Argentina, Australia - PNR,[56] Canada, Faer Oer,[57] Guernsey, Isola di Man, Israele, Jersey, Nuova Zelanda, Svizzera, Uruguay, USA.

Per quanto riguardano gli Stati Uniti, la Commissione ha previsto due Decisioni di esecuzione in merito alla protezione dei dati: "la Decisione di esecuzione UE n. 2016/1250 della Commissione, del 12 luglio, a norma della direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per

[56] "La Direttiva 2016/681 del Parlamento europeo e del Consiglio, del 27 aprile 2016, sull'uso dei dati del codice di prenotazione (PNR) a fini di prevenzione, accertamento, indagine e repressione dei reati di terrorismo e altri reati gravi, si occupa della conservazione (retention) dei PNR. I dati del PNR (Passenger Name Records) sono riconosciuti tra le categorie più sensibili di informazioni personali. Si tratta dei dati compilati dalle agenzie di viaggi, dai vettori aerei e dai tour operator, e che contengono diverse informazioni relative ai passeggeri, tra le quali anche le condizioni mediche e le disabilità, oltre alle preferenze sui pasti, ovviamente i mezzi di pagamento, l'indirizzo di lavoro, l'indirizzo IP se si prenota online e le informazioni personali dei contatti di emergenza."

[57] Faer Oer è un arcipelago di isole vulcaniche rocciose, per l'esattezza sono 18 e sono a governo autonomo che fanno parte del Regno di Danimarca. Si collocano nell'Atlantico del Nord, tra la Norvegia e l'Islanda.

la privacy, ovvero il *"Privacy Shield"*; e la Decisione di esecuzione UE n. 2016/2295 della Commissione del 16 dicembre 2016, che modifica le decisioni nn. 2000/518/CE, 2002/2/CE, 2003/490/CE, 2003/821/CE, 2004/411/CE, 2008/393/CE, 2010/146/UE, 2010/625/UE, 2011/61/UE e le decisioni di esecuzione nn. 2012/484/UE, 2013/65/UE riguardanti l'adeguatezza della protezione dei dati personali da parte di taluni Paesi, a norma dell'articolo 25, paragrafo 6, della Direttiva n. 95/46/CE del Parlamento europeo e del Consiglio, ovvero i PNR".[58] In merito ai PNR, l'UE nel Nuovo Pacchetto sulla protezione dei dati ha predisposto la Direttiva UE n. 2016/681, Direttiva non trattata nel presente elaborato, in quanto per la sua importanza merita un'analisi a se, come già accennato nel Capitolo 2 del presente scritto.

Per quanto riguarda il *Privacy Shield* o il cosiddetto scudo privacy è il nuovo accordo firmato dal Governo americano e la Commissione europea al fine di tutelare i diritti fondamentali dei cittadini dell'UE qualora i loro dati personali vengono trasferiti negli USA. Tale accordo viene a sostituire il vecchio patto che consentiva il trasferimento dei dati personali dei cittadini europei con le società statunitense, il cosiddetto *"Safe Harbor"*, ovvero approdo sicuro. Il 12 luglio 2016 il *Safe Harbor* venne mandato in pensione e rimpiazzato dal *Privacy Shield*, un nuovo meccanismo che riconosce il trasferimento dei dati personali verso gli Stati Uniti. Si tratta di un sistema di autocertificazione che impone alle imprese ed alle organizzazioni, che riceveranno i dati personali appartenenti ai cittadini comunitari, il rispetto di alcuni principi volti a garantire la protezione della privacy. I quali:

- l'assunzione di determinati obblighi attinenti alla modalità del trattamento e al rispetto dei diritti delle persone coinvolte;

- il controllo sulle imprese americane che effettuano trattamento dei dati di cittadini europei verrà svolto dalla *Federal Trade Commission* ;[59]

- l'agire da parte delle società americane conformemente alle pronunce delle Autorità garanti europei;

- il Governo statunitense deve garantire l'inesistenza di attività di monitoraggio indiscriminato.

Qualora venissero violati i diritti fondamentali dei cittadini europei, le Autorità garanti europei provvederanno ad assicurare una tutela effettiva nei loro confronti tramite l'assunzione di strumenti adeguati. Inoltre le Autorità potranno presentare i specifici casi di violazione dei diritti fondamentali dei cittadini UE da parte della società americane dinnanzi la *Federal Trade Commission*, oppure qualora tale violazione fosse stata fatta da

[58] Op. cit. Supra note 8, pp.198-199.
[59] Federal Trade Commission (FTC) – Commissione Federale per il Commercio.

parte di un'autorità di intelligence si rincorre ad un difensore civico (Ombudsman).

In merito al *Privacy Shield*, anche il Gruppo di lavoro "articolo 29" espresse il suo parere, specificando il fatto che: *"si tratta di un meccanismo di autocertificazione per le società stabilite negli USA che intendano ricevere dati personali dall'Unione europea. In particolare, le società si impegnano a rispettare i principi in esso contenuti e a fornire agli interessati adeguati strumenti di tutela, pena l'eliminazione dalla lista delle società certificate ("Privacy Shield List") da parte del Dipartimento del Commercio statunitense e possibili sanzioni da parte della Federal Trade Commission."*[60]

Invece per quanto concerne l'adesione al *Privacy Shield*, tutte le società con lo stabilimento sul territorio statunitense e che sono soggette ai poteri di controllo della *Federal Trade Commission* o del *Department of Transportation*[61] hanno il diritto all'adesione a questo accordo. Dunque le organizzazioni che non sono soggette alla giurisdizione della FTC o del DoT non possono presentare un'autocertificazione ai sensi dello Scudo Privacy.

3.9.3 Trasferimento sulla base dell'adozione da parte del titolare di garanzie adeguate

Qualora mancasse la decisione di adeguatezza da parte della Commissione europea, il trasferimento dei dati verso Paesi extra-UE può avvenire sulla base della predisposizione di garanzie adeguate da parte del titolare del trattamento che intende trasferire dati personali verso Paesi terzi. Si tratta di strumenti giuridici aventi il fine di garantire una tutela adeguata ai cittadini europei. Tali strumenti non richiedono l'autorizzazione dell'Autorità Garante e sono individuati dallo stesso Regolamento all'articolo 46, paragrafo 2:

a) *"uno strumento giuridicamente vincolante e avente efficacia esecutiva tra autorità pubbliche o organismi pubblici;*

b) *le norme vincolanti d'impresa in conformità dell'articolo 47;*

c) *le clausole tipo di protezione dei dati adottate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;*

d) *le clausole tipo di protezione dei dati adottate da un'autorità di controllo e approvate dalla Commissione secondo la procedura d'esame di cui all'articolo 93, paragrafo 2;*

e) *un codice di condotta approvato a norma dell'articolo 40, 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; o*

[60] Op. cit. Supra note 8, cit. pp. 210-211.
[61] Department of Transportation (DoT) – Ministero dei Trasporti

f) *un meccanismo di certificazione approvato a norma dell'articolo 42, unitamente all'impegno vincolante ed esigibile 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."*[62]

Tra gli strumenti giuridicamente vincolanti aventi efficacia esecutiva tra Autorità pubbliche o organismi pubblici si collocano tutti quei accordi internazionali tra Soggetti pubblici europei e Paesi terzi. Al riguardo, il Regolamento specifica al considerando 102 che tali accordi tra l'Unione e i Paesi terzi, i quali disciplinano il trasferimento dei dati personali, includendo le adeguate garanzie, non vengono pregiudicati dal presente Regolamento. L'unica condizione che deve essere rispettata quando si effettuano tali accordi è quella di non incidere sul presente Regolamento o in generale, su qualsiasi altra disposizione del diritto europeo. Inoltre è richiesto il rispetto e la tutela dei diritti fondamentali degli interessati tramite l'adozione di un livello adeguato di protezione.

Per quanto riguarda le norme vincolanti di impresa *(BCR – Binding Corporate Rules)* esse vengono definite dallo stesso Regolamento all'articolo 4, paragrafo 20, come *"le 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 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."*

Il fenomeno della globalizzazione e lo sviluppo dei mercati hanno portato alla nascita dei gruppi multinazionali, i quali ogni anno registrano un elevato numero di scambi di dati personali, il che porta ad avvertire la necessità dell'adozione di una politica intenta a garantire un adeguato livello di protezione. In risposta a questa necessità si sono sviluppate le norme vincolanti d'impresa, che in breve tempo sono diventate lo strumento principale grazie al quale i dati possono circolare liberamente. In sostanza queste *rules* vengono adottate dalla capogruppo – che per regolamento deve essere stabilita nel territorio dell'Unione - sotto forma di un regolamento interno al gruppo multinazionale in materia di privacy. Tale regolamento interno viene sancito tramite la dichiarazione unilaterale della capogruppo e il suo rispetto resta obbligatorio da parte delle società collegate. In altre parole, utilizzando l'espressione inglese, questo regolamento consiste in un serie di clausole (appunto *rules*) che stabiliscono i principi vincolanti (*binding*) in capo a tutte le società facenti parte dello stesso gruppo multinazionale (*corporate*). In base all'esistenza delle BCR il trasferimento dei dati al di fuori dell'UE risulta semplificato.

[62] Articolo 46, paragrafo 2 – GDPR.

Il Regolamento UE n. 2016/679 disciplina le BCR all'articolo 47, prevedendo il loro impiego anche a quelle imprese che pur non facendo parte di un gruppo imprenditoriale, svolgono un'attività economica comune. In quest'ultimo caso esse si individuano con l'espressione di norme vincolanti orizzontali. Inoltre l'articolo 47 sancisce i requisiti che devono essere soddisfatti affinché i dati possano circolare liberamente infragruppo sulla base delle BCR, le quali devono, ai sensi del paragrafo 1:

a. essere giuridicamente vincolanti e applicabili a tutti i membri interessati del gruppo imprenditoriale o delle imprese che svolgono attività economica comune, inclusi i dipendenti;

b. conferire i diritti degli interessati in merito al trattamento dei loro dati personali;

c. soddisfare i requisiti previsti al paragrafo 2 del presente articolo.

I requisiti previsti al paragrafo 2 sono:

a) *"la struttura e le coordinate di contatto del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e di ciascuno dei suoi membri;*

b) *i trasferimenti o il complesso di trasferimenti di dati, in particolare le categorie di dati personali, il tipo di trattamento e relative finalità, il tipo di interessati cui si riferiscono i dati e l'identificazione del paese terzo o dei paesi terzi in questione;*

c) *la loro natura giuridicamente vincolante, a livello sia interno che esterno;*

d) *l'applicazione dei principi generali di protezione dei dati, in particolare in relazione alla limitazione della finalità, alla minimizzazione dei dati, alla limitazione del periodo di conservazione, alla qualità dei dati, alla protezione fin dalla progettazione e alla protezione per impostazione predefinita, alla base giuridica del trattamento e al trattamento di categorie particolari di dati personali, le misure a garanzia della sicurezza dei dati e i requisiti per i trasferimenti successivi ad organismi che non sono vincolati dalle norme vincolanti d'impresa;*

e) *i diritti dell'interessato in relazione al trattamento e i mezzi per esercitarli, compresi il diritto di non essere sottoposto a decisioni basate unicamente sul trattamento automatizzato, compresa la profilazione ai sensi dell'articolo 22, il diritto di proporre reclamo all'autorità di controllo competente e di ricorrere alle autorità giurisdizionali competenti degli Stati membri conformemente RGPD Garante per la protezione dei dati personali all'articolo 79, e il diritto di ottenere riparazione e, se del caso, il risarcimento per violazione delle norme vincolanti d'impresa;*

f) *il fatto che il titolare del trattamento o il responsabile del trattamento stabilito nel territorio di uno Stato membro si assume la responsabilità per qualunque violazione*

delle norme vincolanti d'impresa commesse da un membro interessato non stabilito nell'Unione; il titolare del trattamento o il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità solo se dimostra che l'evento dannoso non è imputabile al membro in questione;

g) *le modalità in base alle quali sono fornite all'interessato le informazioni sulle norme vincolanti d'impresa, in particolare sulle disposizioni di cui alle lettere d), e) e f), in aggiunta alle informazioni di cui agli articoli 13 e 14;*

h) *i compiti di qualunque responsabile della protezione dei dati designato ai sensi dell'articolo 35 o di ogni altra persona o entità incaricata del controllo del rispetto delle norme vincolanti d'impresa all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e il controllo della formazione e della gestione dei reclami;*

i) *le procedure di reclamo;*

j) *i meccanismi all'interno del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune per garantire la verifica della conformità alle norme vincolanti d'impresa. Tali meccanismi comprendono verifiche sulla protezione dei dati e metodi per assicurare provvedimenti correttivi intesi a proteggere i diritti dell'interessato. I risultati di tale verifica dovrebbero essere comunicati alla persona o entità di cui alla lettera h) e all'organo amministrativo dell'impresa controllante del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune e dovrebbero essere disponibili su richiesta all'autorità di controllo competente;*

k) *i meccanismi per riferire e registrare le modifiche delle norme e comunicarle all'autorità di controllo;*

l) *il meccanismo di cooperazione con l'autorità di controllo per garantire la conformità da parte di ogni membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune, in particolare la messa a disposizione dell'autorità di controllo dei risultati delle verifiche delle misure di cui alla lettera j);*

m) *i meccanismi per segnalare all'autorità di controllo competente ogni requisito di legge cui è soggetto un membro del gruppo imprenditoriale o del gruppo di imprese che svolgono un'attività economica comune in un paese terzo che potrebbe avere effetti negativi sostanziali sulle garanzie fornite dalle norme vincolanti d'impresa; e*

n) *l'appropriata formazione in materia di protezione dei dati al personale che ha accesso permanente o regolare ai dati personali."*[63]

[63] Articolo 47, paragrafo 2 – GDPR.

Infine le norme vincolanti d'impresa vengono approvate dall'Autorità Garante competente, in quanto tra i suoi poteri vi è anche quello di ratificare le BCR ai sensi dell'articolo 58, paragrafo 3, lett. j). Le BCR possono essere approvate anche dall'Autorità di controllo capofila in base all'articolo 57, paragrafo 1, lett. s).

Tra le garanzie adeguate, il Regolamento prevede all'articolo 46, paragrafo 2, lett. c) l'adozione della clausole tipo o le *standard model clause*. Esse sono predisposte dalla Commissione e consistono in modelli contrattuali standard sottoscritte sia dall'importatore che dall'esportatore dei dati e vengono generalmente allegate ai contratti di servizio. La Commissione tramite queste clausole standard tutela l'interessato – trasmittente dei propri dati – assicurandoli una garanzia adeguata. Il contenuto delle clausole prevede, da un lato gli obblighi in capo all'esportatore e all'importatore dei dati e dall'altro i diritti dell'interessato, in questo contesto individuato con l'espressione di "terzo beneficiario". A quest'ultimo viene riconosciuta la possibilità di richiedere l'attuazione delle clausole per inadempimento del soggetto importatore od esportatore dei dati ed eventualmente richiedere il risarcimento dei danni al giudice competente.

Le clausole standard non costituiscono una novità introdotta dal GDPR, infatti esse erano già previste nella Direttiva 95/46/CE all'articolo 25, comma 2 e nel Codice Privacy all'articolo 44, lett. b), ma queste disposizioni furono abrogate in seguito a due decisioni prese dalla Commissione: la Decisione della Commissione n. 2001/497/CE del 15 giugno 2011, relativa alle clausole contrattuali tipo per il trasferimento di dati a carattere personale verso Paesi terzi, con Autorizzazione del Garante 10 ottobre 2001 e la Decisione della Commissione n. 2001/16/CE del 27 dicembre 2001, relativa alle clausole contrattuali tipo per il trasferimento di dati personali a incaricati del trattamento residenti in Paesi terzi, con Autorizzazione del Garante del 10 aprile 2002. Successivamente entrambe sono state modificate rispettivamente con la Decisione n. 2004/915/CE del 27 dicembre 2004 si sono apportate delle modifiche alla Decisione n. 2001/497/CE e con la Decisione n. 2010/87/UE del 5 febbraio 2010 è stata modificata la Decisione n. 2001/16/CE.

La novità del Regolamento viene introdotta alla lett. d) (art. 46, paragrafo 2), ovvero alle Autorità di controllo viene data la possibilità di adottare clausole proprie secondo la procedura prevista dal Regolamento all'articolo 93, paragrafo 2.

Per quanto concerne l'elaborazione dei codici di condotta da parte di associazioni e altri organismi rappresentanti le categorie di titolari o responsabili del trattamento, essi trovano approvazione dal Regolamento all'articolo 40, paragrafo 2, lett. j), inoltre il Regolamento sottolinea il fatto che la ragione per cui possono essere adottati i codici di condotta risiede nell'applicazione del presente Regolamento. In merito al trasferimento dei dati verso Paesi

terzi, l'adozione dei codici di condotta può fungere da garanzie adeguate con l'intento di assicurare la tutela degli interessati. Inoltre essi non necessitano di un'autorizzazione da parte dell'Autorità di controllo.

Infine, come garanzia adeguata viene riconosciuto il meccanismo di certificazione approvato ai sensi dell'articolo 42. Il meccanismo di certificazione, così come i codici di condotta, non hanno bisogno di alcuna autorizzazione da parte dell'Autorità di controllo.

Successivamente, all'articolo 46, paragrafo 3 viene sancito che ulteriori garanzie adeguate possono essere costituite da clausole contrattuali private *ad hoc* (art. 46, paragrafo 3, lett. a)) o da accordi amministrativi tra soggetti pubblici (art. 46, paragrafo 3, lett. b)). Contrariamente ai codici di condotta e ai meccaniscmi di certificazione, entrambi gli accordi necessitano di un'autorizzazione da parte dell'Autorità di controllo.

3.9.4 Trasferimento dei dati in deroga agli artt. 45 e 46

Quando non persiste né una decisione di adeguatezza da parte della Commissione né le garanzie adeguate di cui all'articolo 46, il Regolamento all'articolo 49 permette il trasferimento dei dati verso Paesi terzi solo se soddisfate le condizioni seguenti:

a) *"l'interessato abbia esplicitamente acconsentito al trasferimento proposto, dopo essere stato informato dei possibili rischi di siffatti trasferimenti per l'interessato, dovuti alla mancanza di una decisione di adeguatezza e di garanzie adeguate;*

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, solo a condizione che sussistano i requisiti per la consultazione previsti dal diritto dell'Unione o degli Stati membri."*[64]

Se non dovesse persistere nessuna delle condizioni di cui sopra, il trasferimento è possibile se è solo se il titolare del trattamento nutre interessi legittimi e cogenti ed inoltre il trasferimento non deve essere ripetitivo e deve riguardare un numero limitato di interessati. In questo caso, il titolare del trattamento ha l'obbligo di informare del trasferimento dei dati verso Paesi terzi l'Autorità garante.

[64] Articolo 49, paragrafo 1 – GDPR.

Capitolo 4

Modello di valutazione d'impatto Privacy

La valutazione d'impatto sulla protezione dei dati è uno strumento facente parte del gruppo dei cosiddetti *accountability tools*, avente il fine di valutare il rischio inerente al trattamento. Tale rischio è riferito all'interessato e non al titolare del trattamento. Come specifica lo stesso Garante: *[questo rischio] è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (a tal riguardo si vedano i considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito processo di valutazione (artt. 35 e 36, GDPR) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi. All'esito di questa valutazione di impatto, il titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'Autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di autorizzare il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'art. 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento".*[1]

Infatti, il Regolamento generale sulla protezione dei dati individua al suo interno la valutazione d'impatto privacy come un criterio fondamentale, in quanto ha lo scopo di consentire al titolare del trattamento di dimostrare di aver rispettato le normative dettate dal GDPR. Inoltre, l'istituto della *Data Protection Impact Assessment (DPIA)* assume un ruolo centrale nella valutazione dei trattamenti, dal momento che nell'ottica del Regolamento UE n. 679/2016, l'Autorità di controllo interviene principalmente successivamente alle determinazioni assunte in modo autonomo dal titolare del trattamento (art. 36), quindi un intervento ex post.

[1] Guida allapplicazione del Regolamento europeo in materia di protezione dei dati personali - Garante Privacy.

4.1 Il Parere del Gruppo di Lavoro Art. 29 del 4 aprile 2017 riguardante la DPIA

Il Gruppo di Lavoro Articolo 29 ha pubblicato delle Linee Guida in materia di valutazione d'impatto sulla protezione dei dati in data 4 aprile 2017, modificate ulteriormente in data 4 ottobre 2017. Secondo il WP29, richiamando quanto previsto all'articolo 35 del GDPR:

"Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24). In altre parole, una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità."[2]

Secondo il Regolamento UE n. 679/2016 la valutazione d'impatto sulla protezione dei dati va effettuato ogniqualvolta un trattamento comporti un rischio elevato per i diritti e le libertà delle persone interessate. Questo costituisce un obbligo in capo al titolare del trattamento, il quale svolge la valutazione d'impatto sulla protezione dei dati prima di iniziare il trattamento. Una volta individuati i rischi annessi al trattamento e adottate le misure tecniche ed organizzative necessarie per mitigare l'impatto del trattamento, se queste ultime sono ritenute insufficienti, ovvero il rischio residuale per i diritti e le libertà degli interessati resti elevato, il titolare consulta l'Autorità di controllo.

Sempre nelle Linee guida, il WP29 sottolinea l'importanza della valutazione di impatto sulla protezione dei dati riferita al tema della responsabilizzazione, in quanto rappresento uno degli strumenti che esprime la responsabilizzazione dei titolari nei confronti dei trattamenti da questi eseguiti. Questo è un valido motivo per cui è buona prassi effettuare la valutazione d'impatto sempre e comunque, anche se non vi risiedono i criteri per cui deve essere intrapresa obbligatoriamente. Inoltre, grazie a questo strumento, il titolare può ricavare indicazioni molto utili e di notevole importanza nel prevenire incidenti futuri, permettendo di realizzare la protezione dei dati fin dalla fase di progettazione (la cosiddetta *Privacy by Design*) di qualsiasi trattamento. Tuttavia, questo non include l'obbligatorietà,

[2] Linee-guida del Gruppo Articolo 29 in materia di valutazione di impatto sulla protezione dei dati (WP248).

in effetti nelle Linee guida viene precisato quando la valutazione d'impatto sia obbligatoria, oltre a quanto previsto all'articolo 35 del Regolamento. L'obbligatorietà scatta quando un trattamento presenta un elevato rischio per i diritti e le libertà degli interessati. Ma cosa si intende per rischio elevato? Ovvero quando il titolare deve effettuare la valutazione d'impatto? Per rispondere a queste domande spontanee, il WP29 fornisce nove criteri che si devono considerare come un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, pur non trovando collocamento all'interno dell'elenco di cui all'articolo 35, paragrafo 3, da lettera a) a lettera c), in quanto tale elenco non è esaustivo, incompletezza sottolineata dallo stesso Regolamento nella frase introduttiva dell'articolo 35, paragrafo 3, esattamente attraverso le parole *"In particolare"*. In base al Parere del WP29 si devono considerare i seguenti nove criteri:

1. "**Valutazione o assegnazione di un punteggio**, inclusiva di profilazione e previsione, in particolare in considerazione di "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'impresa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

2. **Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente**: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che "hanno effetti giuridici" o che "incidono in modo analogo significativamente su dette persone fisiche" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;

3. **Monitoraggio sistematico**: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo35, paragrafo 3, lettera c)) . Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a

conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

4. **Dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

5. **Trattamento di dati su larga scala**: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

    a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;

    b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;

    c. la durata, ovvero la persistenza, dell'attività di trattamento;

    d. la portata geografica dell'attività di trattamento;

6. **Creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato;

7. **Dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio a causa dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

8. **Uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita "in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;

9. Quando il trattamento in sé **"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"** (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno."[3]

[3] Ibidem.

Una volta che il titolare abbia individuato che il trattamento soddisfi due di questi criteri, egli deve condurre la valutazione di impatto sulla protezione dei dati, in quanto, secondo il WP29, il trattamento che soddisfa due o più criteri di cui sopra, molto probabilmente incorpora un rischio elevato per i diritti e le libertà dei soggetti interessati. Tuttavia, nulla vieta al titolare del trattamento dei dati effettuare la valutazione di impatto qualora il trattamento soddisfi uno solo di questi criteri, anzi come affermato precedentemente, il WP29 invita i titolari a provvedere all'attuazione della DPIA sempre.

Il WP29 predispone un elenco di casi in cui non è richiesta la valutazione di impatto sulla protezione dei dati (si veda pag. 14-15, Linee Guida del WP29 in materia di DPIA del 4 aprile 2017 e modificate il 4 ottobre 2017), tra cui: *"quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 1[4])"*[5]. Invece, in merito ai trattamenti già in essere, non sempre vi è l'obbligo di condurre una valutazione di impatto sulla protezione dei dati. Questo dovere scaturisce quando vi è stata una variazione dei rischi, ovvero *"la natura, l'ambito di applicazione, il contesto, le finalità del trattamento, i dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative ecc. sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati"*.[6]

Inoltre, nelle Linee guida il Gruppo di Lavoro Articolo 29, mette in risalto che la valutazione di impatto deve essere interpretata come un processo soggetto a revisione continua e non come una adempimento una tantum, dal momento che è un processo continuo che va aggiornato durante il ciclo di vita del trattamento. Per quanto concerne i soggetti incaricati ad effettuare la valutazione di impatto sulla protezione dei dati, le Linee guida individua tali soggetti nella figura del titolare e quella del responsabile del trattamento, se vi è designato. Questi mettono in atto il processo, tenendo conto del parere del *Data Protection Officer*, il quale vigila sullo sviluppo della *Data Protection Assessment Impact*.

Un altro punto fondamentale riguarda la metodologia utilizzata nello svolgimento della DPIA. Le Linee guida non forniscono un modello preciso da seguire nella fase di attuazione della valutazione di impatto sulla protezione dei dati, essa può essere svolta attraverso

[4]"[...] Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi." – Art. 35, paragrafo 1.

[5]Linee Guida del WP29 in merito alla DPIA

[6]Ibidem.

l'impiego di metodologie diverse, purché vengano seguiti criteri comuni. Dunque la DPIA è uno strumento flessibile e la sua attuazione è modulabile, questo sta a significare che ciascun titolare è libero di progettare e attuare una DPIA adatta ai propri trattamenti. Tale flessibilità viene sottolineata nel Regolamento UE n. 679/2016 al considerando 90: *"[...]è opportuno che il titolare del trattamento effettui una valutazione d'impatto sulla protezione dei dati prima del trattamento, per valutare la particolare probabilità e gravità del rischio."* In effetti, il Regolamento generale sulla protezione dei dati fornisce un quadro generico per quanto concerne la progettazione e lo svolgimento di una valutazione di impatto, stabilendo i requisiti che devono essere rispettati. Dunque spetta a ciascun titolare ad integrare le predisposizioni dettate dal Regolamento per poter attuare un DPIA che meglio si adatti al livello di rischi del proprio trattamento e che gli permetta di dimostrare la conformità al GDPR.

Ad ogni modo, ai sensi dell'articolo 35, paragrafo 7, tenendo conto anche dei considerando 84 e 90, una valutazione di impatto deve avere almeno le seguente caratteristiche:

a) *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*

b) *"una valutazione della necessità e proporzionalità dei trattamenti";*

c) *"una valutazione dei rischi per i diritti e le libertà degli interessati";*

d) *"le misure previste per:*

   - *"affrontare i rischi";*
   - *"dimostrare la conformità al presente regolamento".*

Per avere le caratteristiche di cui sopra, il WP29 illustra il seguente processo iterativo generico per lo svolgimento di una DPIA:

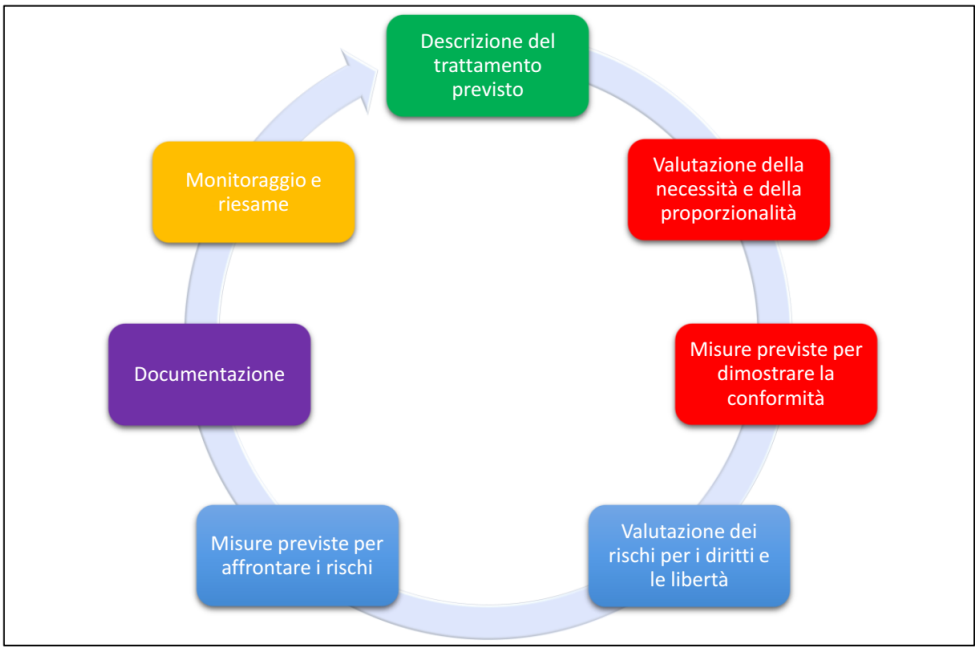


Figura 4.1: *Processo Iterativo generico per lo svolgimento della DPIA*

Si vuole sottolineare il fatto che il processo appena esposto è iterativo, questo significa che ciascuna delle fasi può essere riesaminata più volte prima che venga portata a termine la valutazione di impatto sulla protezione dei dati.

4.2 L'attività di DPIA

Per quanto riguarda l'attività di valutazione di impatto sulla protezione dei dati, il WP29 propone un modello di valutazione di impatto, all'interno dell'allegato 2 al Parere del 4 aprile 2017, modificato successivamente il 4 ottobre 2017. In particolare, il modello viene proposto tenendo conto del contenuto dell'articolo 35, paragrafo 7 del GDPR, quindi delle caratteristiche che deve avere la valutazione d'impatto sulla protezione dei dati.

Come primo elemento, la DPIA deve prevedere, ai sensi dell'art. 35, paragrafo 7, lett. a), una descrizione sistematica del trattamento. Per adempiere a tale richiesta, si devono considerare la natura, la portata, il contesto e la finalità del trattamento. Inoltre, si deve fornire una descrizione dei dati personali raccolti, individuati i destinatari e il periodo di conservazione. Di notevole importanza è la descrizione funzionale del trattamento. Non di meno è l'individuazione delle risorse su cui sono trattati i dati personali, come hardware, software, mezzi cartacei, persone o reti. Tale descrizione sistematica del trattamento va fatta rispettando i codici di condotta approvati (art. 35, paragrafo 8).

Successivamente alla lett. b) dell'art.35, paragrafo 7, viene sancito che l'attività della DPIA deve valutare i principi di necessità e proporzionalità rispetto alle finalità del trattamento. Nel perseguire questo fine vanno identificare le misure necessarie per adattarsi ai principi di proporzionalità e di necessità, considerando le finalità specifiche, esplicite e legittime, la liceità del trattamento, l'adeguatezza, pertinenza e limitazione dei dati, la limitazione della durata di conservazione. Inoltre, si devono individuare le misure contribuenti a garantire i diritti degli interessati tenendo conto dell'informativa fornita all'interessato, diritto di accesso, diritto alla portabilità dei dati, diritti alla rettifica, cancellazione, all'opposizione, alla limitazione del trattamento; dei destinatari; dei responsabili; delle garanzie sul trasferimento internazionale e della consultazione preventiva.

Secondo la lett. c), la valutazione di impatto sulla protezione dei dati deve occuparsi della gestione dei rischi per i diritti e le libertà delle persone interessate. Per gestire tali rischi si deve condurre un'analisi circa l'origine, la natura, la particolarità e la gravità dei rischi. Inoltre è di fondamentale importanza la considerazione del punto di vista dei soggetti interessati per ciascun rischio, come ad esempio l'accesso illegittimo, la modifica indesiderata e la perdita dei dati. In base al considerando 90 si deve prendere in esame le fonti di rischio, i potenziali impatti per i diritti e le libertà delle persone in caso di accesso illegittimo, modifica indesiderata e perdita dei dati; le eventuali minacce che potrebbero portare all'accesso illegittimo, alla modifica indesiderata o alla perdita dei dati. Si deve tener presente la probabilità e gravità che si verifichi la minaccia. Infine, le misure che si intendono adottare per affrontare tali rischi (art.35, paragrafo 7, lett. d)).

Per avere un quadro completo del modello di valutazione di impatto sulla protezione dei dati, il Regolamento generale sulla protezione dei dati prevede i soggetti coinvolti nel giudizio di valutazione sempre all'articolo 35, che come già accennato al paragrafo precedente, essi sono il DPO, se designato, al quale viene richiesto un parere sullo svolgimento della DPIA (art. 35, paragrafo 2) e gli interessati, i quali forniscono le loro opinioni in merito al trattamento previsto (art. 35, paragrafo 9).

4.3 La corretta attuazione di un modello di DPIA conforme al GDPR

Il punto fondamentale su cui viene centrato il nuovo Regolamento sulla protezione dei dati, come è stato detto più volte, è il concetto di responsabilizzazione. E questo fa sì che le organizzazioni per essere conformi al GDPR, rispettando i vari principi ispiratori del GDPR, tra cui il principio dell'*accountability*, devono adottare un approccio basato sulla continua valutazione del rischio.

La corretta attuazione di un modello conforme al Regolamento UE n. 679/2016 obbliga le organizzazioni a revisionare l'approccio burocratico e cartaceo utilizzato ante GDPR, soprattutto in Italia, al fine di salvaguardare la privacy, ai sensi del GDPR. Fondamentalmente si devono tener presenti 3 elementi per poter mettere in atto i profondi cambiamenti richiesti dal nuovo Regolamento. In primo luogo, bisogna implementare un modello di gestione privacy *"PDCA-thinking"* (si veda la figura 2 riportata di seguito), che deve essere integrato con gli altri sistemi di gestione aziendali, messi in atto per garantire all'organizzazione la conformità a schemi di Certificazione volontari, come SGQ per ISO 9100, SGSI per ISO 27001, ecc. In secondo luogo, il personale che vi opera all'interno dell'organizza-

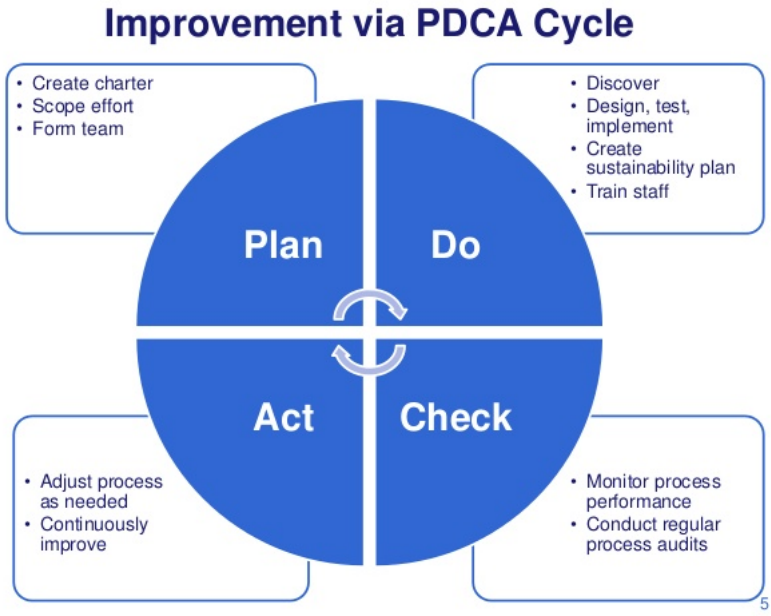


Figura 4.2: *Modello di gestione Privacy PDCA-thinking*

zione deve essere al corrente dei rischi aziendali per poter mantenere nel lungo periodo la *compliance* richiesta. Può sembrare banale, ma anche se si è adottato il miglior modello di gestione privacy che possa esistere, se le persone che vi lavorano all'interno dell'azienda non sono pienamente consapevoli dei rischi aziendali, non potrà essere garantita la conformità alle disposizioni dettate dal Regolamento. Concernente a questa questione il Consiglio d'Europa ha sviluppato il concetto di sensibilizzazione (*awareness-raising*) del personale, sottolineando la notevole importanza della diffusione della consapevolezza in merito al tema della privacy a tutti i livelli aziendali.

Infine, il terzo elemento consiste nell'introdurre all'interno dell'azienda uno strumento in grado di rendere sistematica la valutazione del rischio privacy. Tale strumento deve essere flessibile per potersi adattare a diversi livelli di rischi, dato che ogni trattamento

è diverso da altri, inoltre deve essere potente ed efficace per implementare un modello di valutazione di impatto sulla protezione dei dati conforme al GDPR. Questo strumento è proprio il processo di DPIA, che non solo è in grado di adempiere agli obblighi dettati dal Regolamento, ma anche capace di integrarsi nel ciclo di Enterprise Risk Management, dal momento che si basa su framework standard di Risk Management.[7]

Ritornando sul tema della responsabilizzazione, il focus dell'intero Regolamento, il processo di DPIA costituisce uno strumento fondamentale, come sottolinea lo stesso WP29, in quanto prevede le registrazioni necessarie a sostenere il principio dell'*accountability*, aiutando il titolare a dimostrare l'adozione di misure idonee a garantire il rispetto delle predisposizioni europee in materia di protezione dei dati. Il fatto che la DPIA venga fatta prima di effettuare un trattamento fa sì che essa costituisca la base per la *Privacy by Design*, perché rende possibile l'individuazione e l'implementazione delle misure di sicurezza idonee per i prodotti e i servizi che trattano dati personali, consentendo così al titolare ed al responsabile di affrontare la questione della protezione dei dati prima che il prodotto o il servizio venga emesso sul mercato. Tale valutazione preventiva consente di dare concretezza alle strategie aziendali relative al rischio di impresa, grazie alla gestione consapevole del rischio residuo basata su un processo di analisi a più livelli.

Infine, si vuole chiarire che il processo di DPIA non è un processo IT. Solitamente, si interpreta in maniera errata, pensando che esso si riferisca alla protezione del dato, in realtà il punto centrale si focalizza sul rispetto della privacy dell'interessato e ciò porta ad ampliare l'analisi centrandola sugli impatti sulla persona e sul suo diritto all'autodeterminazione informativa.

L'efficacia del processo viene determinata dal fatto che il processo stesso sia *"buit-in"* nel sistema di gestione per la privacy che si sta progettando. In più deve essere progettato in modo che sia da una lato iterativo, e dal altro deve essere attivato in maniera automatica da consentire al responsabile del trattamento di individuare i rischi privacy e di valutare tali rischi e adottare le misure necessarie per eliminarli o quanto meno mitigarli. Infine, se il rischio residuo è comunque elevato, il titolare del trattamento deve consultare l'Autorità di controllo, prima di iniziare il trattamento (art. 36, GDPR – "Consultazione preventiva").

4.3.1 Gli Standard utilizzati per la valutazione della sicurezza dei dati

Come già accennato precedentemente, il Regolamento generale sulla protezione dei dati non definisce un modello obbligatorio da seguire quando si effettua la valutazione di impatto sulla protezione dei dati, benché si limita a fornire gli elementi di base che un titolare

[7] M. SOFFIENTINI, *Privacy-protezione e trattamento dei dati*, Assago, Ipsoa, 2018, pp.318-319.

del trattamento deve considerare quando predispone la DPIA.

Bisogna spostarsi nel Nuovo Continente per trovare le origini dei primi standard per valutare la sicurezza dei dati risalenti ai primi anni '80. Invece, la prima pubblicazione avente per argomento i criteri concernenti la valutazione della sicurezza dei dati gestiti da sistemi informatici risale al 1983 ad opera del Dipartimento della Difesa (USA) ed è identificabile come lo standard TCSEC *(Trusted Computer Security Evaluation Criteria)*, oppure anche con la connotazione di *Orange Book*. In Europa bisogna aspettare gli anni '90 per assistere alla pubblicazione dei criteri ITSEC *(Information Technology Security Evaluation Criteria)*, utilizzati nella valutazione della sicurezza dei prodotti e dei sistemi IT.
La sostanziale differenza tra i criteri statunitensi e quelli europei risiede nel fatto che lo standard TCSEC (USA) è centrato sulla riservatezza delle informazioni, invece lo standard ITSEC (UE) hanno lo scopo di valutare la capacità del sistema nell'adottare misure idonee a garantire la terna RID[8] associata alle informazioni, attraverso l'impiego di sette gradi di valutazione diversi, ovvero valutare le misure applicate ai prodotti o ai servizi per determinare il grado di confidenza di sicurezza del target (ToE-Target of Evaluation). I criteri ITSEC furono successivamente rimpiazzati dai Common Criteria, i quali sono divenuti standard internazionale ISO/IEC 15408-2:1999. I Common Criteria curano gli aspetti tecnici relativi alla sicurezza, escludendo quelli organizzativi e logistici. A dare uno standard completo che includesse anche questi aspetti fu il British Standards Institute (BSI), che pubblicò nel 1995 lo standard britannico BS 7799, da cui deriva l'attuale ISO 27001. Quest'ultimo standard definisce i requisiti per attuare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e si basa su un approccio olistico, ovvero che tacca sia gli aspetti tecnici, sia quelli logistici, nonché quelli organizzativi.
Oltre all'approccio olistico su cui si sviluppano gli standard della famiglia ISO 27K, essi costituiscono una svolta per le organizzazioni aderenti, in quanto permettono a queste di realizzare un proprio modello per la gestione della sicurezza delle informazioni, inoltre, grazie al meccanismo della certificazione è possibile dimostrarne l'attuazione. Lo scopo di questi standard è quello di condurre le organizzazioni nello seguire un approccio strutturato durante l'impiego delle misure efficaci per contrastare il rischio della perdita delle caratteristiche RID delle informazioni gestite da un sistema informatico, e qualora fosse necessario, anche l'adozione dei *cyberattack*.[9]

[8] RID sta per Riservatezza, Integrità e Disponibilità.
Secondo l'Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione (ISCOM): "Un prodotto informatico sicuro deve garantire:

- la Riservatezza, cioè impedire che le informazioni siano accessibili a persone non autorizzate;
- l'Integrità, cioé impedire la modifica non autorizzata delle informazioni;
- la Disponibilità, cioè assicurare l'accesso alle informazioni da parte del personale autorizzato."

[9] Con il termine *"cyberattack"*, riferito all'ambito della sicurezza informatica, si intende: "è una qua-

Oltre a questo strumento, alle organizzazione viene fornito un ulteriore aiuto proveniente dal NIST *(National Institute of Standards and Tecnology)* per le organizzazioni statunitense e dalla ENISA *(European Network and Information Security Agency)* per quelle europee.
Il NIST predispone di continuo aggiornamenti per quanto riguarda le politiche, le procedure e le linee guida del Governo Federale statunitense allo scopo di apportare delle migliorie nell'ambito della sicurezza dei sistemi IT e delle reti dati. Tuttavia, l'applicazione del framework NIST richiede un impegno non da poco per quanto concerne l'impostazione e l'attuazione del modello per la sicurezza delle informazioni.
L'ENISA (Agenzia europea a supporto della sicurezza dei dati e delle reti) funge da *competence center* di sicurezza informatica europea e ha l'obiettivo fondamentale di sostenere i Paesi membri nella gestione della sicurezza dell'informazione. Per adempiere a tale scopo, essa pubblica numerosi studi relativi ai framework, agli strumenti di Risk Management ed infine, alle minacce alla sicurezza delle informazioni. Queste pubblicazioni costituiscono un insieme di indicazioni che risultano di cruciale importanza per le organizzazioni che intendono mettere in atto un proprio modello di sistema di gestione del rischio, dal momento che invita le organizzazioni, in fase di *assessment*, a considerare tutte le minacce aventi la possibilità di insidiare i propri attivi.

4.4 Il processo di *Data Protection Impact Assessment*

Il processo di *Data Protection Impact Assessment* consiste nel trovare il giusto compromesso tra la complessità degli elementi presi in considerazione quando viene eseguita la valutazione d'impatto sulla protezione dei dati e il bisogno di disporre uno strumento concreto, efficace e flessibile, in modo tale da adattarsi alla particolarità del titolare o del responsabile del trattamento, qualora fosse designato. Pur non avendo a disposizione alcun modello da cui poter trarre ispirazioni per poi attuare uno proprio, esistono delle indicazioni fornite dal Gruppo di Lavoro Art. 29 nelle citate Linee Guida. Le quali lasciano molta libertà al titolare del trattamento, in quanto il processo di DPIA non deve essere inteso come un processo a se stante, benché deve integrare la gestione dei rischi privacy all'interno del modello di *Enterprise Risk Management System* dell'organizzazione. Tuttavia, nell'allegato 1 alle Linee guida, il WP29 fornisce dei generici *framework* di DPIA predisposti da varie Autorità di controllo, e questi sono:

lunque manovra, impiegata da individui od organizzazioni anche statali, che colpisce sistemi informativi, infrastrutture, reti di calcolatori e/o dispositivi elettronici personali tramite atti malevoli, provenienti generalmente da una fonte anonima, finalizzati al furto, alterazione o distruzione di specifici obiettivi violando sistemi suscettibili. Tali azioni sono classificabili in *cyber campaign*, guerre cibernetiche o *cyberterrorismo* a seconda del contesto. Gli attacchi informatici spaziano dall'installazione di *spyware* su di un PC fino a tentativi di demolizione delle infrastrutture di intere nazioni."

1. "FR: Privacy Impact Assessment (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015.

2. DE: modello per la protezione dei dati standard, V.1.0 - versione di prova, 201631.

3. ES: Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD), Agencia española de protección de datos (AGPD), 2014.

4. UK: Conducting privacy impact assessments code of practice, Information Commissioner's Office (ICO), 2014."[10]

In più, vengono forniti 2 esempi di framework specifici:

1. "Privacy and Data Protection Impact Assessment Framework for RFID Applications [Quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID].

2. Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems [Modello per la valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti]."

Oltre a questi framework, si trovano sui siti ufficiali delle Autorità strumenti per la DPIA e *tool* di *assessment Privacy* o di *self-assessment*. Tali strumenti costituiscono dei punti cruciali che dovrebbero essere studiati al fine di effettuare una valutazione di impatto aggiornata.

Infine, per avere il quadro completo, si devono prendere in considerazione anche le Linee guida pubblicate dalla ISO *(International Organization for Standardization)* in merito all'attuazione di una DPIA, ovvero gli standard ISO/IEC[11] 29134:2017, che propongono:

a) Un processo per il *privacy impact assessment*,

b) Una struttura ed i relativi contenuti del report del DPIA, i quali aiutano il titolare del trattamento nell'adempimento del principio di responsabilizzazione.

Le presenti Linee Guida apportano un enorme contributo alle organizzazione che intendono condurre la valutazione di impatto sulla protezione dei dati, in quanto permettono il collegamento tra i passaggi più delicati del processo e uno standard preimpostato, facendo sì che quest'ultimo possa essere migliorato nel tempo attraverso un continuo monitoraggio, al fine di renderlo in perfetto equilibrio con la cultura di sicurezza adottata dall'organizzazione, garantendone l'efficienza. Per quanto riguarda l'efficacia, ovvero valutare l'aspetto

[10] Linee-guida del WP29 in materia di valutazione di impatto sulla protezione dei dati (WP248), Allegato 2.

[11] IEC è l'acronimo di *International Electrotechnical Commission* (Commissione Elettrotecnica Internazionale).

economico, giustificando il denaro speso per la protezione dei dati, si prendono in considerazione due indici: il ROPI *(Return on Privacy Investment)* e il ROSI *(Return on Security Investment)*, non sono altro che il conosciuto ROI *(Return on Investment)*. Grazia alla DPIA sarà possibile individuare le misure di sicurezza adottate per annullare, o quantomeno mitigare, il rischio rilevato. Ovviamente le misure intraprese hanno un costo e di conseguenza ci si aspetta una loro efficacia. Sempre il processo della DPIA si occupa del monitoraggio dei costi sostenuti e dei risultati ottenuti in modo tale da poter effettuare un'analisi *bottom-up* dei costi Privacy.[12]

4.4.1 Le fasi del processo di DPIA

Per quanto attiene alle fasi del processo di DPIA, anche in questa sede è utile far riferimento alle Linee Guida pubblicate dal Gruppo del Lavoro Articolo 29, il quale fornisce una schematizzazione dei principi base.

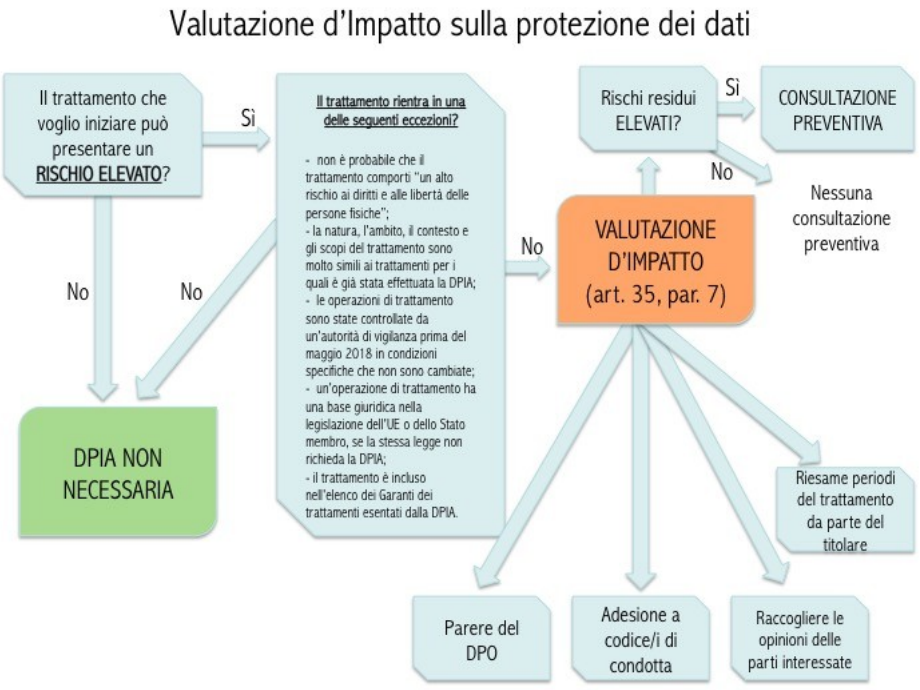


Figura 4.3: *Principi base della DPIA secondo il WP29*

L'inizio del processo di valutazione d'impatto sulla protezione dei dati è segnato dalla sola idea di un nuovo trattamento. Quindi, come è stato affermato precedentemente, la valutazione di impatto viene messa in atto, ancor prima che il trattamento sia realizzato. Inoltre, per essere in linea con il Regolamento UE n. 679/2016, il processo è iterativo e

[12]Op. cit. Supra note 7, pp. 323-324.

deve essere ripreso qualora si verificassero modifiche considerevoli del trattamento che possono aumentare il livello di rischio, pregiudicando i diritti e le libertà dei soggetti interessati.

Per quanto riguarda i ruoli, non c'è ombra di dubbio che il *Data Protection Officer* ha il compito di governare il processo *in toto*. Tuttavia, bisogna considerare anche gli altri attori coinvolti nello svolgimento della DPIA, e per tale motivo si deve prendere in considerazione la matrice RACI, o anche detta matrice di assegnazione responsabilità. Tale matrice ha la funzione fondamentale di assegnare i ruoli agli attori coinvolti per ciascuna attività, non a caso l'acronimo RACI incorpora i 4 possibili ruoli che un attore può giocare, per ogni attività. Infatti:

- R=*Responsible*: esegue l'attività;
- A=*Accountable*: responsabile del risultato dell'attività. Mentre gli altri ruoli non richiedono l'assegnazione per ciascuna attività, l'*accountable* lo richiede;
- C=*Consulted*: è in collaborazione con il *Responsible* nell'esecuzione dell'attività;
- I=*Informed*: è colui che viene informato sugli esiti e sull'esecuzione dell'attività; la sua selezione viene fatta secondo la logica del *need-to-know*.

Fase 1: Valutare la necessità di condurre una DPIA Questa fase è stata già trattata nel momento in cui si è parlato delle Linee Guida pubblicate dal Gruppo di Lavoro Art. 29. Riprendendo I casi in cui il titolare del trattamento dei dati è tenuto ad effettuare una valutazione di impatto sono illustrati all'articolo 35, paragrafo 3, GDPR, inoltre bisogna considerare i 9 criteri esposti nelle Linee Guida del WP29, la soddisfazione di almeno 2 di questi criteri implica la necessità in capo al titolare di predisporre un processo di DPIA.

Fase 2: Valutare la conformità al Regolamento e al principio di liceità Al fine di essere conforme al GDPR, il titolare del trattamento e, qualora sia designato, anche il responsabile adottano delle misure tecniche e organizzative idonee previste all'articolo 35, paragrafo 7, lett. d) e al considerando 90, ovvero le misure che contribuiscono alla proporzionalità e necessità del trattamento e misure che contribuiscono ai diritti delle persone interessate. Oltre a queste misure è necessario tener presente anche il principio di liceità (articolo 6, GDPR) e valutare se vengono applicate o meno le 6 condizioni di liceità previste all'articolo 6, paragrafo 1.

Fase 3: Descrizione del Trattamento Il focus di questa fase è il ciclo di vita dell'informazione, ovvero la Raccolta, l'Archiviazione, l'Utilizzo ed infine la Cancellazione.
Questa fase costituisce un punto cruciale, in quanto la descrizione del trattamento evidenzia quale informazione viene usata, a quale finalità e chi può accedervi. Grazie ad una esatta comprensione di come e dove circolano i dati è possibile sottolineare i rischi ai quali

incorrono e quindi poter fare importanti considerazioni sugli attori, sulla *supply chain*, sul trasferimento di dati verso Paesi terzi, sugli *asset* in gioco, ecc.

In più, nell'effettuare la descrizione del trattamento si deve rispettare la conformità al GDPR, ai sensi dell'articolo 35, paragrafo 7, lett. a), e secondo il considerando 90 bisogna tener conto della natura, della portata, del contesto e delle finalità, ed infine devono essere rispettati i codici di condotta approvati in base all'articolo 35, paragrafo 8.

Una volta che si è definita la natura, ovvero la tipologia dei dati personali trattati si può passare allo *step* successivo, cioè alla valutazione dei possibili impatti per i diritti e le libertà fondamentali delle persone in caso di accesso illegittimo (R), modifica indesiderata (I) e perdita dei dati personali o la loro indisponibilità (D).
In conclusione, dopo che sono stati definiti i dati e gli *asset* coinvolti si può fare la descrizione dei flussi dei dati personali.

Fase 4: Valutazione del Rischio Durante la quarta fase vengono individuati i rischi verso gli interessati. È fondamentale considerare nell'insieme tutte le tipologie di rischi relativi all'organizzazione, non solo i rischi privacy. Al fine di individuarli è consigliabile utilizzare i metodi già adottati all'interno dell'organizzazione e tener presente delle indicazioni fornite al riguarda da parte del Garante, del Gruppo di Lavoro Articolo 29 o da parte di fonti attendibili, come organismi di certificazione o agenzie. Una volta individuati i rischi, questi vanno valorizzati, ovvero vanno misurati e classificati a seconda delle categorie a cui si riferiscono, e questa procedura viene effettuata tramite il proprio modello dell'organizzazione, che può essere di tipo quantitativo, qualitativo o misto. Tutte queste operazioni formano, nell'ottica di responsabilizzazione, una Registrazione SGP (Sistema di Gestione Privacy).

Punto di notevole rilievo nella valutazione del rischio è costituito dal fatto che è necessario prendere in considerazione tutti i fattori coinvolti (trattamento, dati personali, *stakeholders*, *asset*, figure privacy, impatto, minacce, vulnerabilità, rischio, probabilità, ecc.) e le possibili relazioni tra di essi, in quanto rendono complicata l'attività di valutazione. Per renderla meno stressante, si incoraggiano le organizzazioni di intraprendere un approccio sistematico e strutturato per garantire l'efficacia e l'efficienza del modello predisposto, ad esempio, tale modello potrebbe essere in accordo con la ISO 15408:2005.

Oltre all'adozione di un modello efficace ed efficiente, la valutazione dei rischi necessita di una corretta individuazione delle minacce che presentano un'alta probabilità di aver successo sugli *asset* coinvolti nel trattamento. Principalmente gli *asset* coinvolti sono quelli indicati dal WP29, ovvero hardware e software di proprietà dell'interessato oppure gene-

rali, rete, siti, persone, documenti cartacei e canali di trasmissione dei documenti.

Ad ogni modo, bisogna tener presente che non è possibile identificare tutte le minacce, il consiglio suggerito alle organizzazioni è quello di continuare a utilizzare i propri database delle minacce e combinare quelle costituenti un pericolo per le tre caratteristiche fondamentali dei dati personali, ovvero: la Riservatezza, l'Integrità e la Disponibilità. Tuttavia, non esistono solo le caratteristiche RID, ed infatti il Regolamento sottolinea in più punti che non bisogna soffermarsi solamente alla tutela del dato in quanto tale, benché adottare un approccio olistico e considerare quindi la libertà e il rispetto della privacy delle persone interessate.

Fase 5: Gestione del Rischio In questo *step* l'organizzazione definisce le attività da avviare per eliminare o quanto meno mitigare i rischi, anzi l'obbiettivo è quello di diminuire il livello del rischio ma non azzerarlo così da non avere più alcun impatto privacy. Il focus è sulla privacy e non sulla sicurezza del dato, per approcciarsi correttamente al principio di *privacy by design*.

Per quanto riguarda la quantificazione del rischio, la si può esprimere in funzione della gravità delle conseguenze (C) e della probabilità o della frequenza con cui si verificano le conseguenze (P), ovvero:

$$R = f(C, P) \tag{4.1}$$

dove R rappresenta la variabile dipendente, il rischio.

Tuttavia, è buona prassi quantificare il rischio residuo in seguito all'applicazione delle misure di mitigazione dei rischi individuati precedentemente. In questo caso la variabile endogena viene esplicata oltre dalle due variabili esogene introdotte in precedenza anche da una terza, ovvero la vulnerabilità residua in seguito all'applicazione dei controlli necessari (I). Dunque la funzione diventa:

$$R = f(C, P, I). \tag{4.2}$$

Solitamente, tutte le attività intraprese durante la fase della valutazione del rischio risultano necessarie al fine di:

- acquisire consapevolezza a tutti i livelli aziendali del grado di rischio cui sono sottoposti gli *asset* informativi *(Risk Identification, Risk Analysis)*;

- stabilire se il livello di rischio si classifica nei limiti dell'accettabilità o se vi è bisogno di fare la richiesta di un trattamento secondo i criteri di accettazione definiti a livello aziendale *(Risk Evaluation)*.

Ritornando sulla funzione del rischio determinata precedentemente cogliendone il significato. Stabilire la funzione del rischio f vuol dire arrivare alla specificazione di un modello di esposizione dei trattamenti a determinati pericoli che mette in relazione l'entità del danno atteso, cioè l'Impatto, con la probabilità che tale danno si verifichi. Normalmente ci possono essere tre scenari di impatto privacy:

1. Danno Reputazionale (DR) si verifica quando trattamenti di dati personali invasivi della privacy o violazione di dati personali, la cosiddetta *data breach*, comportano la delegittimazione da parte degli *stakeholders*, consumatori o clienti e compromettono la reputazione della società sul mercato.

2. Violazioni di norme di legge (VN): si tratta dei trattamenti illeciti o *data breach*. In questo caso la violazione viene punita con sanzioni civili o amministrative o addirittura penali o con il pagamento di penali contrattuali;

3. Richieste di Risarcimento (RR): gli interessati effettuano le richieste di risarcimento qualora il trattamento dei dati personali sia illecito o si sia verificata una violazione dei dati personali.

Dunque la valutazione degli impatti gioca un ruolo importante nella fase di gestione del rischio, in quanto stabilisce le possibili conseguenze sia per gli interessati che per l'organizzazione, nel momento in cui dovessero venir meno uno o più dei requisiti di sicurezza caratteristici dei dati personali, ovvero le caratteristiche RID. La perdita di tali caratteristiche è dovuta a:

- accesso in mancanza dell'autorizzazione o divulgazione ingiustificata, privando l'interessato della Riservatezza (R);

- alterazione accidentale o indebita delle informazioni, compromettendo l'Integrità dell'informazione (I);

- indisponibilità delle informazioni, riportando ripercussioni sulla Disponibilità dell'informazione (D).

Al fine di identificare l'impatto su un solo dato trattato (DATOn) si deve considerare il valore massimo risultante per l'insieme dei requisiti di sicurezza caratteristici dei dati personali (RID) rispetto a ciascun scenario di impatto:

$$I(DATOn) = Max(Rn, In, Dn). \tag{4.3}$$

Se invece si vuole determinare l'impatto del Trattamento I(T), si deve considerare l'insieme degli impatti su ciascun dato personale del trattamento, ovvero (DATO1, DATO2, ..., DATOn) e massimizzare gli impatti trovati precedentemente per i singoli dati trattati, quindi:

$$I(T) = Max[I(DATO1), I(DATO2), \ldots, I(DATOn)] \tag{4.4}$$

È consigliabile l'utilizzo della scala di valutazione suggerita dallo standard internazionale ISO/IEC 29134:2017 al fine di stimare gli impatti sia per quanto riguarda il singolo dato sia per quanto concerne il Trattamento.

Un altro fattore che influenza notevolmente la determinazione del Rischio è la probabilità di successo delle minacce sugli *asset*. Anche in questo caso lo standard internazionale ISO 29134 fornisce un modo qualitativo per la valutazione della probabilità di successo delle minacce. Al livello 1 la probabilità di successo delle minacce è trascurabile, in quanto "l'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto non sembra possibile per le fonti di rischio selezionate (ad esempio, il furto di documenti cartacei archiviati in una stanza protetta da un lettore di badge e un codice d'accesso)".[13] Al livello 2 la probabilità che le minacce abbiano successo è limitata. Successivamente al terzo livello la probabilità è significativa ed infine al quarto livello di probabilità raggiunge il suo massimo, dato che l'esecuzione di una minaccia sfruttando le proprietà delle risorse di supporto risulta facile per le fonti di rischio selezionate, un esempio è quello del furto dei documenti cartacei tenuti in posti aperti al pubblico.

Dalla combinazione di questi due fattori – l'impatto del Trattamento e la probabilità di successo delle minacce – si riesce ad indentificare il Rischio del trattamento. In merito, la ISO 29134 mette a disposizione la seguente *Privacy Risk Map*:

[13] Op. cit. Supra note 7, p. 341, Figura 16: ISO – Livello di probabilità di successo delle minacce privacy.

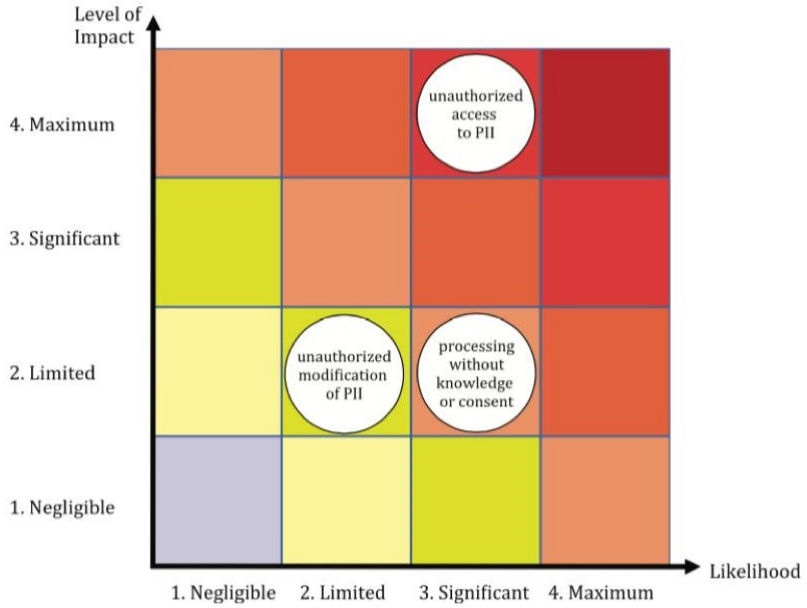


Figura 4.4: ISO 29134:2017 – *Privacy Risk Map*

Il risultato è una scala quali-quantitativa ISO ottenuto dal prodotto tra l'Impatto e il Livello di probabilità di successo. Tale risultato viene associato al livello di rischio del trattamento. Si individuano 4 livelli di rischio:

- **Trascurabile**: raramente una minaccia ha successo sul trattamento e quindi l'impatto risulta trascurabile. Il prodotto tra l'impatto è la probabilità va da 1 a 4.
- **Limitato**: vi è la possibilità che una minaccia abbia successo sul trattamento e produca impatti non trascurabili. Il prodotto tra l'impatto e il livello di probabilità va da 6 a 8;
- **Significativo**: una minaccia ha successo sul trattamento con conseguenza sull'impatto significative se non addirittura massime. Il prodotto va da 9 a 12;
- **Massimo**: la probabilità che una minaccia abbia successo e produca un impatto sul trattamento è molto alta.

Solitamente si valuta se il rischio è accettabile o meno (RA).[14] Fatta tale considerazione, si passa all'implementazione del piano di interventi, dando la priorità ai casi con un alto livello di rischio stimato, ovvero il livello del rischio stimato è superiore del livello di rischio accettabile (R>RA).

[14]RA= rischio accettabile.

La domanda che sorge spontanea è la seguente: come si gestiscono i rischi una volta determinate le componenti del rischio?

Normalmente, le modalità di gestione dei rischi sono quattro:

1. *Accettare*: valutati i costi e i benefici si decide di accettare il rischio;
2. *Ridurre*: si adottano delle contromisure sostenibili al fine di mitigare il rischio;
3. *Trasferire*: traslare il rischio a soggetti terzi, come clienti/fornitori, *outsourcer*, società di assicurazione, ecc.;
4. *Rimuovere*: non si effettuano quei trattamenti che presentano un livello elevato di rischio, in questo modo lo si evita.

Proprio durante la gestione dei rischi che si deve decidere se il rischio residuo rientra nei limiti dell'accettabilità o meno, qualora esso dovesse risultare elevato, nonostante il tentativo da parte del titolare del trattamento di *"[...] attenuare mediante misure opportune in termini di tecnologia disponibile e costi di attuazione, prima del trattamento si dovrebbe consultare l'Autorità di controllo"*.[15] Inoltre, la consultazione preventiva viene trattata all'articolo 36, paragrafo 1 del Regolamento UE n. 679/2016.

Tuttavia, il focus è sul come il titolare individua le misure idonee al fine di ridurre il rischio della violazione dei dati *(data breach)* e ridurre anche l'impatto che possano avere al verificarsi degli incidenti sugli interessati da un lato, ma dal altro anche sull'organizzazione stessa. Per affrontare tale questione è necessario un approccio strutturato in grado di fornire un vasto elenco di controlli da installare. A tale scopo è stato sviluppato lo standard internazionale ISO/IEC 29151.

Fase 6: Piano di azioni Il piano di azioni costituisce un elemento fondamentale nell'ottica dell'*accountability*, in quanto permette di determinare un piano condiviso che incorpora le misure da adottare, le responsabilità di attuazione e di verifica e di assunzione dell'Alta Direzione, la consapevolezza del rischio residua a tutti i livelli aziendali. Inoltre, grazie all'operazione di stima dei costi relativi alle misure intraprese, e quindi ai Costi della Privacy, permette di valutare l'efficacia delle misure adottate attraverso l'indice ROPI *(Return On Privacy Investment)*.

Fase 7: Monitoraggio del Trattamento I rischi Privacy sono dei rischi aziendali a tutti gli effetti e per questo motivo vanno monitorati e valutati nell'ambito di gestione dei rischi aziendali, costituiscono elementi dell'*Enterprise Risk Management System* e perciò

[15] Considerando 84 del GDPR.

devono essere portati all'attenzione dell'Alta Direzione.

Anche in questa fase come nella precedente, si mette in atto il *built-up* dei costi sostenuti durante l'adozione delle misure di sicurezza identificate nella fase di gestione del rischio. Infine si valuta l'efficacia di tali misure, più esse sono efficaci più l'indice ROPI risulta alto.

4.5 Il Modello di valutazione d'impatto sulla protezione dei dati

Sulla base delle indicazioni fornite dalle Linee guida del Gruppo di Lavoro articolo 29 in merito alla DPIA, si cercherà di concretizzare un modello di valutazione di impatto privacy basato sul rischio[16], composto da quattro sezioni tra loro distinte: la check-list, le informazioni aggiuntive, la sintesi e il masterplan degli interventi.

4.5.1 La Check-list

La Check-list costituisce la prima sezione del modello di DPIA e a sua volta è formata da undici colonne: il tipo di verifiche, gli adempimenti, i riferimenti normativi, il rischio potenziale, l'indice di rischio potenziale, l'attività di verifica, la valutazione del presidio, rischio residuo assoluto, l'indice di rischio residuo, le annotazioni ed infine le criticità individuate in data gg/mm/aaaa.

Nella colonna denominata "adempimenti" viene riportato un elenco di elementi di cui il titolare del trattamento dovrà tenere conto al fine di essere conforme al Regolamento UE n. 2016/679, indicandone nella seconda colonna i "riferimenti normativi". Proseguendo verso destra, si trovano le colonne denominate rispettivamente il "rischio potenziale" e "l'indice di rischio potenziale" aventi natura quantitativa e devono essere calcolati per ogni elemento considerato della colonna degli "adempimenti". Il loro calcolo avviene tramite il modello per identificare e valutare i rischi adottato dall'organizzazione in questione, quindi varia a seconda dell'organizzazione. Successivamente al calcolo del rischio potenziale e del suo indice si effettua la verifica per ogni adempimento e si riporta nella colonna denominata appunto "attività di verifica". Nel proseguire ci si imbatte nelle colonne che permettono di valutare il presidio, e di calcolare il "rischio residuo assoluto" e "l'indice di rischio residuo". Per quanto riguarda le ultime due colonne, le "annotazioni" e le "criticità individuate in data [...]", queste servono al titolare post trattamento, in quanto la DPIA va sempre monitorata e aggiornata.

[16] Si vuole sottolineare il fatto che il rischio trattato è un rischio di non conformità, ovvero il rischi di incorrere in sanzioni giudiziarie o amministrative in mancanza dell'ottemperanza di leggi, regolamenti o norme di autoregolamentazione, che spesso conducono al rischio reputazionale. Tale tipologia di rischio appartiene alla categoria dei rischi "non quantificabili" ovvero "difficilmente quantificabili", poiché non esistono delle metodologie per valutarli quantitativamente: per questo la loro valutazione può non essere immediata.

Gli adempimenti

In merito agli adempimenti si sono considerati in totale ventotto e per ciascuno di essi si è cercato di individuare il riferimento normativo. I primi cinque adempimento si focalizzano sulla base legale del trattamento e i principi ad esso applicabili, il riferimento normativo è costituito dagli articoli 5, ovvero i principi applicabili al trattamento dei dati personali, trattati in modo dettagliato nel capitolo 3 della presente dissertazione, e l'articolo 6, paragrafo 1, ovvero la liceità del trattamento, anche questa tematica è stata affrontata nel capitolo 3, ma bisogna sottolineare l'importanza del consenso, che come viene definito all'articolo 4 al numero 11), si tratta di *"qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."* In mancanza del consenso da parte dell'interessato, il trattamento si ritiene illecito.

Proseguendo con l'elenco degli adempimenti, il sesto adempimento pone l'attenzione sull'interessato considerando una serie di elementi come le condizioni per il consenso, qualora sia stato dato da esso nel trattamento dei propri dati, previste all'articolo 7, l'informativa concernete la finalità per cui sono stati raccolti i dati qualora siano stati raccolti presso l'interessato (art.13) o presso terzi (art.14), la modalità d'esercizio dei propri diritti previsti agli artt. 15-22 (art.12). Con riguardo al consenso si tiene a precisare che qualora il trattamento trattasse categorie particolari di dati personali, ci deve essere il consenso. Inoltre, ponendo l'attenzione sull'informativa e sulla raccolta del consenso, l'organizzazione deve attrezzarsi di una funzione aziendale responsabile dell'aggiornamento e della predisposizione dell'informativa sulla privacy e della raccolta del consenso, che devono essere necessariamente in forma scritta e stampate, in modo tale da riuscire a dimostrare che l'interessato sia stato informato e abbia ricevuto tutta la documentazione in merito al trattamento dei dati personali preventivamente. Nel momento in cui i dati vengono raccolti, il titolare del trattamento deve prevedere ad informare l'interessato della finalità e della modalità del trattamento; dei suoi diritti e della modalità di esercitarli; l'identità e i dati di contatto del titolare del trattamento, e se designati, del responsabile del trattamento e del responsabile della protezione dei dati; dei destinatari dei dati personali, inclusi i destinatari esteri, e in tali casi specificando l'esistenza dei requisiti previsti agli articoli 46 o 47 o 49, incluse le garanzie adeguate indicando la modalità per ottenere una copia di tali garanzie o il luogo dove sono state rese disponibili; i dati di contatto e l'identità del titolare, e se designati del rappresentante e del DPO, dello Stato estero; del fatto che il processo decisionale sia automatizzato o meno.

Al settimo adempimento vengono considerati tutti gli Incaricati del trattamento e l'ambito di trattamento, I riferimenti normativi sono rispettivamente gli articoli 28 e 29 che

trattano rispettivamente la figura del responsabile del trattamento e il trattamento sotto l'autorità del titolare del trattamento o del responsabile del trattamento. In merito alla nomina del responsabile del trattamento si deve verificare che essa sia avvenuta tramite atto giuridico in forma scritta ai sensi dell'articolo 28, paragrafi 3, 4 e 9. Inoltre al responsabile vengono fornite da parte del titolare del trattamento tutte le istruzioni di cui al presente articolo. Anche gli incaricati devono essere individuati e nominati con procedura simile, e dati a loro tutte le istruzioni circa i poteri e le responsabilità a loro conferite. È di fondamentale importanza l'esistenza di una procedura aziendale che si occupi di verificare l'adeguatezza con cui avviene l'individuazione e la nomina degli incaricati, nonché la ripartizione delle mansioni, poteri e responsabilità ad essi conferiti allo scopo di evitare l'accesso a dati personali da parte di personale non autorizzato.

Per quanto concerne il trasferimento dei dati verso Paesi extra-UE, è argomento dell'ottavo adempimento che trova come riferimenti normativi negli articoli 44, 45, 46. Innanzitutto si effettua una verifica se i dati sono soggetti al trasferimento verso Stati al di fuori dell'UE. Qualora la risposta è positiva si individua se vengono fornite adeguate garanzie, ovvero se sussistono le seguente circostanze:

a) Il Paese terzo offre un'adeguata tutela riconosciuta dall'UE;

b) Nel caso degli Stati Uniti, l'organizzazione ricevente deve aver aderito allo Scudo Privacy (Privacy Shield);

c) Se non dovessero sussistere nessuna delle precedenti circostanze, bisogna verificare che i dati personali trattati godono della stessa tutela garantita negli Stati membri UE e i diritti degli interessati sono rispettati.

Inoltre determinare il fatto che il trasferimento dei dati personali verso una Stato extra-UE è stato possibile grazie ad una decisione di adeguatezza da parte della Commissione o sulla base dell'esistenza delle garanzie adeguate. In più, i titolari del trattamento o il responsabile del trattamento delle organizzazioni che si trovano in una Stato extra-UE devono aver designato un Rappresentante nell'UE. Tale figura può essere una persona fisica o una persona giuridica con l'incarico appunto di rappresentanza del Titolare o del Responsabile del trattamento in merito al GDPR. La nomina del Rappresentante rappresenta un obbligo qualora il trattamento non è occasionale, prevede l'utilizzo su larga scala di categorie particolari di dati personali o di dati relativi a condanne penali e reati e registra un'alta probabilità che tale trattamento presenti un rischio per i diritti e le libertà delle persone fisiche, tenuto conto della natura, del contesto, dell'ambito di applicazione e delle finalità del trattamento. Nelle circostanze contrarie a quanto appena detto l'obbligo decade. Lo stesso succede se il Titolare extra-UE è un'Autorità pubblica o un organismo pubblico. Un altro punto da precisare in merito alla figura del Rappresentante è che la sua nomina non deresponsabilizza il Titolare extra-UE, infatti contro quest'ultimo possono essere

mosse azioni legali qualora si fossero verificate inosservanze ed episodi di non conformità al Regolamento generale sulla protezione dei dati.

In seguito, l'organizzazione deve verificare l'utilizzo di categorie particolari di dati personali e se questi vengono trattati, verificare se il loro utilizzo avviene in modo sistematico o in certe occasioni.
Il riferimento normativo in materia di categorie di particolari di dati personali è l'articolo 9 del GDPR, il quale vieta il trattamento di dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale. Tale divieto viene esteso ai dati genetici, dati biometrici o relativi alla salute o all'orientamento o vita sessuale della persona. Ma l'articolo 9, paragrafo 2 elenca un serie di casi per cui tale divieto decade, il più noto è l'esistenza del consenso esplicito da parte dell'interessato *"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."*[17]

Successivamente, al decimo adempimento si pone l'attenzione sui dati relativi alle condanne penali o reati e come riferimento normativo si considera l'articolo 10 del GDPR e l'articolo 2-octies del Codice della privacy. L'articolo 10 sancisce l'ammissibilità del trattamento di tali dati che deve avvenire esclusivamente sotto il controllo dell'Autorità pubblica – la quale deve tenere un registro delle condanne penali – o in presenza dell'autorizzazione da parte del diritto dell'Unione o degli Stati membri che preveda garanzie adeguate per i diritti e le libertà degli interessati. In questo caso l'organizzazione deve verificare se raccoglie questa particolare categoria di dati, il modo con cui essa avviene – sistematico od occasionale, – la loro portata, la finalità, nonché la presenza dell'autorizzazione in merito al trattamento di dati relativi a condanne penali e reati.

Nel proseguire con l'analisi degli adempimenti i prossimi quindici sono dedicati al Rischio, analizzando in special modo tre categorie di rischio privacy: l'Accesso illegittimo ai dati, le modifiche indesiderate ai dati personali ed infine la perdita degli stessi. Nello svolgimento dell'analisi si deve considerare:

- l'esistenza degli eventi che impattano negativamente sui diritti e le libertà delle persone;

- la frequenza con cui tali eventi si verificano, ovvero la probabilità con cui un potenziale rischio si converta in un vero e proprio danno;

- le conseguenze del danno, quindi la gravità;

[17] Articolo 9, paragrafo 2, lett. a) – GDPR.

- l'attuazione delle misure idonee al fine di attenuare i rischi;

- il costo in termini economici per contrastarlo.

Il livello di sicurezza dell'organizzazione, che si tratti di un'azienda ospedaliera, una banca o un call center, si rivelerà idoneo nel momento in cui esso è in grado di affrontare le tipologie di rischio di cui sopra. Il compito del titolare è quello di valutare i potenziali rischi e in base all'esito di tale valutazione il titolare provvederà nell'adozione delle misure tecniche ed organizzative in grado di attenuare i rischi individuati. In altre parole, quello che deve fare il titolare del trattamento è garantire un livello di sicurezza adeguato attraverso le misure adeguate, le quali devono raggiungere lo stato di equilibrio tra i rischi da affrontare e lo stato dell'arte e i costi di attuazione.

Per quanto riguarda le misure di sicurezza da intraprendere, il GDPR lascia libero arbitrio al titolare, nel senso che non elenca le misure di sicurezza che il titolare dovrebbe adottare al fine di garantire un adeguato livello di sicurezza, ma fornisce ad esso dei parametri per la loro individuazione. Il fatto di non fornire l'elenco delle misure di sicurezza da adottare si giustifica attraverso il principio dell'*accontability*, che delinea l'intera normativa europea sulla protezione dei dati personali.
Dunque la concentrazione cade sui parametri, che il legislatore europeo fornisce al titolare, utili nella fase dell'individualizzazione delle misure di sicurezza da attuare per fronteggiare i rischi.
In primis si considera lo stato dell'arte, ovvero il parametro che tiene conto della disponibilità tecnologica che ha l'organizzazione, in riferimento ai vari strumenti che può impiegare a tale scopo.
Successivamente si prendono in considerazione i costi di attuazione, cioè le risorse occorrenti per mettere in funzione gli strumenti tecnologici.
In seguito, si devono considerare la natura, l'oggetto, il contesto e le finalità del trattamento. Ricordando che:

- quando si esplicita la natura del trattamento questo significa che si spiega il fatto se il trattamento prevede o meno la divulgazione a terzi dei dati raccolti;

- l'oggetto del trattamento invece si riferisce alla tipologia dei dati che verranno trattati, ovvero se il trattamento riguarda dati sensibili o dati relativi alla salute o dati relativi a condanne penali e reati o dati di minori o semplicemente dati comuni;

- il contesto è determinato dalla qualità e dalla dimensione del trattamento all'interno del mercato in cui opera;

- la finalità invece rappresenta lo scopo aspirante del titolare. Tale fine può essere di natura istituzionale, legale, economica o sociale.

Infine, ci sono altri due parametri da prendere in considerazione, ovvero la probabilità[18] e il grado di gravità[19] per i diritti e le libertà delle persone fisiche.
Dunque durante il processo di Valutazione d'impatto sulla protezione dei dati personali, il titolare del trattamento deve considerare tutti questi elementi al fine di adottare le misure di sicurezza necessarie per garantire un livello adeguato di sicurezza per i diritti e le libertà delle persone fisiche.

Ritornando alla check-list, i primi cinque adempimenti, ovvero dall'undicesimo al quindicesimo, si concentrano sulle fonti di rischio riferite all'accesso illegittimo ai dati e trovano fondamento normativo nell'articolo 32. Ai sensi del quale si devono considerare i rischi derivanti dall'accesso illegittimo ai dati personali trattati, conservati o divulgati a terzi nella valutazione del livello di sicurezza adeguato. Chi si occupa di tale valutazione deve verificare quale sia la fonte del rischio inerente all'accesso illegale o accidentale ai dati. Questa fonte può essere sia umana che non umana. Come fonte umana di rischio può essere ad esempio un tecnico informatico, che pur non avendo l'accesso autorizzato ai dati, lui effettua comunque l'accesso a dei archivi informatici grazie alle sue conoscenze tecnologiche. Una fonte non umana invece potrebbe essere costituita da un fenomeno naturale catastrofale che riporta conseguenze disastrose per l'ufficio dedicato ai trattamenti.

Successivamente vengono analizzati i potenziali impatti sui diritti e le libertà delle persone fisiche in seguito all'accesso illegittimo ai dati. Tale analisi deve essere soggetta a continui aggiornamenti.

Al tredicesimo adempimento vengono analizzate le minacce sulla base delle quali è possibile determinare ex ante un accesso illegale ai dati personali.

Il penultimo e l'ultimo elemento si focalizzano sulla probabilità e sulla gravità che il rischio attinente all'accesso illegittimo ai dati si realizzi. Mentre la probabilità rappresenta la possibilità che il rischio si realizzi ed è dipendente dal livello di vulnerabilità delle risorse di contrasto alle minacce e della capacità delle fonti di rischio di sfruttare tali vulnerabilità, la gravità considera l'entità del rischio.
Sostanzialmente il compito dell'incaricato alla valutazione del rischio di accesso illegale o accidentale ai dati personali risiede nel condurre un analisi in merito e accertarsi che tale

[18] La probabilità intesa come il rapporto tra occasioni in cui il rischio è diventato danno e la totalità della ricorrenza delle condotte rischiose, ovvero la possibilità che un rischio si concretizzi e dipenda dal livello di vulnerabilità delle risorse di contrasto alle minacce e della capacità delle fonti di rischio di sfruttare tali vulnerabilità.

[19] Per gravità si intende la gerarchia del bene giuridico oggetto dell'attentato. Inoltre il grado di gravità può essere riferito alla misurazione in termini di costi sostenuti al fine di ripristinare la situazione antecedente al verificarsi dell'evento dannoso e di risarcimento del soggetto danneggiato. Dunque la gravità considera l'entità del rischio.

analisi sia sempre aggiornata.

Dal sedicesimo al ventesimo adempimento viene posta l'attenzione sulle modifiche indesiderate di dati e dal ventunesimo al venticinquesimo sulla perdita dei dati. Come precedentemente si fa riferimento all'articolo 32 del GDPR, che, sempre in merito alla valutazione dell'adeguato livello di sicurezza, tiene considerazione i rischi derivanti dalla modifica, dalla distruzione e dalla perdita dei dati, sia che questi si verifichino in modo accidentale che illegale. Anche in questo caso vengono condotte delle analisi aventi per contenuto: le fonti di rischio, gli impatti potenziali sui diritti e le libertà delle persone fisiche le minacce, le probabilità e la gravità del rischio.

In seguito si sono aggiunte volutamente nella check-list delle informazioni aggiuntive sulla base delle quali viene determinata la necessità di effettuare la Valutazione d'impatto sulla protezione dei dati (DPIA). Queste informazioni aggiuntive sono costituite da tre elementi: i primi due hanno come riferimento normativo l'articolo 35, nonché il Considerando 89, mentre l'ultimo l'articolo 35, paragrafo 7 e il Considerando 9.

Il primo dei tre adempimenti si pone la domanda se l'organizzazione impiega nuove tecnologie nello svolgimento del trattamento e, qualora la risposta risultasse positiva, l'incaricato sarà tenuto a verificare la presenza delle misure idonee per affrontarlo. La domanda è di vitale importanza, in quanto l'utilizzo di nuove tecnologie nell'effettuare il trattamento comporta un rischio elevato per i diritti e le libertà delle persone fisiche, il che implica automaticamente lo svolgimento della *Data Protection Impact Assessment*, come stabilito all'articolo 35, paragrafo 1.

In seguito, l'incaricato deve verificare se l'organizzazione effettui trattamenti su larga scala e, anche in questo caso, se abbia le misure adatte per affrontarlo. Ricordando che, ai sensi dell'articolo 35 anche i trattamenti su larga scala implicano un rischio elevato il che significa che il titolare del trattamento ha l'obbligo di effettuare la Valutazione d'impatto sulla protezione dei dati. Un altro punto cruciale gioca la definizione del concetto "larga scala"[20], la quale deve essere precisa e puntuale ancor prima di mettere in atto la DPIA.

Per quanto concerne l'ultimo adempimento della Check-list, questo pone l'attenzione sulle misure di sicurezza che l'organizzazione dovrebbe adottare per mitigare il rischio. Il riferimento normativo in questo caso è l'articolo 35, paragrafo 7, il quale delinea il contenuto della Valutazione, e il Considerando 91. Infatti, per adempiere all'articolo sopra citato, l'incaricato deve fare un serie di verifiche, tra cui:

[20]Concetto che viene approfondito all'interno del Considerando 91, GDPR.

- Verificare l'esistenza di funzioni aziendali responsabili della adozione e aggiornamento di misure di sicurezza nel trattamento dei dati;
- Verificare l'esistenza e l'adeguatezza di una procedura interna che preveda l'adozione di misure di sicurezza finalizzate a ridurre al minimo i rischi di distruzione o perdita dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta;
- Verificare che i dati personali oggetto di trattamento siano custoditi e controllati, anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo i rischi;
- Verificare l'esistenza e l'adeguatezza di istruzioni per la gestione sia della raccolta, sia del trattamento dati da fornire agli operatori di filiale (e non solo);
- Si deve valutare il livello di conoscenza dei dipendenti in termini di GDPR per far sì che essi trattino i dati in conformità alle disposizioni di legge;
- Verificare eventuali codici di condotta a cui si ha aderito.

Un tema molto ricorrente all'interno del GDPR, che però non è stato incluso all'interno della Check-list, riguarda la profilazione. Come viene definita all'articolo 4, num. 4: *"La «profilazione»: 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."* Dunque la profilazione è utile a costruire un profilo dell'interessato che verrà utilizzato per l'assunzione di decisioni. Dal momento che tratta categorie particolari di dati personali, tale tipologia di trattamento è vietata in base dell'articolo 9. Ma vi è proprio una norma apposita che vieta la profilazione ed è l'articolo 22. Infatti l'articolo 22 riconosce all'interessato il diritto di non essere sottoposto a una decisione fondata solamente su un trattamento automatizzato, che produca effetti giuridici nei suoi confronti o che incida significativamente sulla sua persona.
Affinché tale divieto venga derogato, devono sussistere le seguenti condizioni:

a) La decisione derivante da un trattamento automatizzato è necessaria per l'esecuzione o la conclusione di un contratto tra l'interessato e il titolare del trattamento;
b) Tale decisione è autorizzata dal diritto UE o dallo Stato membro cui è soggetto il titolare, il quale deve adottare misure di sicurezza idonee per garantire i diritti e le libertà degli individui, e in merito a tali misure si veda il considerando 71;
c) La decisione è basata sul consenso esplicito dell'interessato.

4.5.2 Informazioni aggiuntive

La sezione successiva alla Check-list denominata "informazioni aggiuntive" costituisce una parte descrittiva del modello che va considerata insieme al documento quantitativo analizzato al paragrafo precedente al fine di mettere a disposizione dei terzi un'analisi completa, trasparente e dettagliata del trattamento sotto esame. Oltretutto, lo stesso Regolamento al Considerando 39 sottolinea l'importanza del principio di trasparenza, ovvero il fatto che il titolare metta a disposizione delle persone fisiche soggette al trattamento tutte le informazioni concernenti quest'ultimo. Infatti gli interessati devono aver ben presente quali siano i rischi, le norme, le garanzie e i diritti in merito al trattamento stesso, nonché le finalità, la natura, l'oggetto e i destinatari. Oltre ad informare gli interessati, questa sezione è utile a coloro che andranno a volgere un'analisi sulla DPIA. Grazie ad una serie di domande alle quali l'incaricato è tenuto a rispondere, si viene a contestualizzare in maniera completa il trattamento.

La prima domanda riguarda la descrizione del trattamento. L'incaricato è tenuto a descrivere brevemente il trattamento, indicando le finalità, l'ambito di applicazione, la natura, nonché le problematiche che esso comporta.

La seconda domanda ha come focus i Responsabili del trattamento, i Contitolari e le loro rispettive responsabilità. La figura del Responsabile del trattamento è di fondamentale importanza, in quanto il responsabile tratta i dati personali di persone fisiche per conto del Titolare. Il responsabile del trattamento può essere sia una persona fisica che una persona giuridica, può essere un dipendente così come una persona esterna all'organizzazione, inoltre il suo rapporto con il Titolare è delineato da una atto contrattuale. Come statuisce l'articolo 28, la sua designazione avviene appunto tramite contratto, e durante tale procedura gli vengono impartiti i compiti e le responsabilità, nonché una serie di indicazioni, quali: le tipologie di dati personali trattati, le categorie degli interessati, la durate del trattamento, i fini, la natura, la diffusione a terzi, ecc. Sempre ai sensi dell'articolo 28, il Responsabile può designare un sub-Responsabile, previa autorizzazione da parte del Titolare, autorizzazione che deve essere necessariamente in forma scritta. Anche in questo caso il rapporto tra il Responsabile e il sub-responsabile è regolato da contratto. Inoltre si vuole sottolineare il fatto che qualora il sub-responsabile non adempie correttamente ai propri obblighi, dinanzi al Titolare risponde il Responsabile. Per quanto concerne i Contitolari, essi sono definiti all'articolo 26, sulla base del quale si ha la contitolarità quando due o più titolari determinano in maniera congiunta le finalità e i mezzi del trattamento. È importante stabilire, tramite accordo interno, i rispettivi compiti e le rispettive responsabilità. Oltre a delineare i compiti e le responsabilità dei Contitolare, l'accordo designa anche un punto di contatto per gli interessati, dal momento che il suo contenuto deve essere messo a disposizione degli interessati.

Successivamente viene chiesto all'operatore se sono stati adottati degli standard di trattamento quali codici di condotta o certificazione. Sia i codici di condotta che le certificazioni sono strumenti molto importanti nel processo di Valutazione di impatto sulla protezione dei dati, perché permettono agli interessati di capire se vi è o meno un adeguato livello di tutela dei dati fornito dai titolari. L'adozione da parte del titolare di questi standard non è obbligatoria, tuttavia l'adesione ad essi implica la conformità al GDPR, in special modo nel processo di Valutazione di impatto sulla protezione dei dati. Infatti, l'Autorità di controllo prende in considerazione dell'adesione ai codici di condotta o alle certificazione da parte del Titolare nel momento in cui valuta se la DPIA è stata effettuata in maniera corretta.

In seguito, alla quarta domanda viene chiesto di indicare le varie tipologie di dati personali soggette al trattamento. Spetta al Titolare il compito di indicare se tratta dati personali comuni o dati appartenenti a categorie particolari, come ad esempio dati relativi alla salute, dati relativi alle condanne penali e reati, dati finanziari o patrimoniali, ecc. Tenendo conto che se i dati trattati appartenessero a categorie particolari, devono sussistere le condizioni di cui all'articolo 9, paragrafo 2. Inoltre si devono indicare le finalità del trattamento.

La quinta domanda pone l'attenzione sui destinatari dei dati personali, indicandone se sono persone fisiche o giuridiche, se sono autorità pubbliche, e in special modo se sono sul territorio UE o extra-UE. Di notevole importanza è quest'ultima considerazione, in quanto se i destinatari risiedono in un Paese terzo, il Titolare del trattamento deve specificare se il trasferimento dei dati avviene in quanto bassato su una decisione di adeguatezza da parte della Commissione o sulle garanzie adeguate come ad esempio le norme vincolanti d'impresa o su deroghe al sussistere di certe situazioni.

Successivamente viene chiesto di indicare le misure di supporto ai dati personali. Queste possono essere sotto forma cartacea o sotto forma elettronica, come i software, i hardware, ecc.

La settima domanda invece chiede all'incaricato di indicare le misure di sicurezza che contribuiscono a garantire un adeguato livello di tutela ai dati personali. Tra queste vi sono:

- La cittografia, ovvero il metodo con il quale si riesce a far sì che i dati siano indecifrabili in assenza di una chiave di lettura. Molto utile in quanto permette di prevenire il rischio di accesso ai dati illegittimo, che può avvenire per mano di personale non auto-

rizzato. Qualora si fa uso di questo metodo, si deve fornire una descrizione dei mezzi impiegati per cittografare i dati, e delle procedure per gestire le chiavi cittografiche;

- La pseudonimizzazione, ovvero una tecnica che non permette l'attribuzione dei dati ad un certo individuo in mancanza di informazioni aggiuntive. Inoltre viene utilizzata anche un'altra tecnica che viene identificata con il nome dell'anonimizzazione. Questa intende cancellare dai dati personali la componente identificativa. Qualora venga utilizzata quest'ultima metodologia è necessario fornire anche i meccanismi su cui si è bassata e le garanzie adottate al fine di fronteggiare una possibile reidentificazione. In più, nell'attuare questa tecnica si deve seguire un approccio definito in base agli utilizzi previsti. In merito, il Gruppo di Lavoro articolo 29 predispone tre criteri di valutazione della validità di un approccio:

  1. Individuazione, ovvero verificare se in seguito all'anonimizzazione il soggetto resta ancora distinguibile all'interno di un gruppo;
  2. Correlabilità, ossia verificare l'esistenza di una correlazione tra il soggetto e un insieme di dati tra loro diversi;
  3. Deduzione, ovvero la possibilità di dedurre informazioni su un certo soggetto.

  Dunque, affinché un dato sia considerato anonimo devono sussistere queste tre condizioni. Qualora mancasse una delle tre caratteristiche, sarà necessario condurre un'analisi dei rischi di reindentificazione in modo dettagliato. Tale analisi permette di verificare l'anonimato dei dati presi in esame.
  Per quanto concerne la pseudonimizzazione, essa è diversa dall'anonimizzazione, in quanto si basa sul fatto che le informazioni aggiuntive siano conservate separatamente dalle informazioni principali e protette da misure di sicurezza tali da non poter ricondurre le informazioni aggiuntive ad un soggetto identificabile. Quindi è una tecnica che funge da supporto all'anonimizzazione in quanto è in grado di attenuare il rischio di correlare più dati tra di loro.

- Il partizionamento, è una tecnica avente il fine di diminuire la possibilità di correlazione tra i dati personali e di un loro sbilanciamento. Anche questa tecnica richiede la descrizione del criterio e dei mezzi impiegati a tal fine;

- L'archiviazione dei documenti cartacei, ovvero le politiche riguardanti la stampa, l'archiviazione, la condivisione dei documenti cartacei contenenti i dati personali ed infine la distruzione di essi;

- L'archiviazione computerizzata, ovvero le politiche riguardanti l'archiviazione informatica dei dati;

- Il controllo degli accessi logici, ovvero un sistema in grado di identificare l'accesso ai dati dei vari profili degli utenti. In questo caso è necessario dare una descrizione in

merito alla modalità con cui sono definiti e attribuiti i profili agli utenti-dipendenti, includendo anche i mezzi di autentificazione;

- La tracciabilità, in riferimento agli eventi e alla gestione dei relativi log: Il Titolare sarà tenuto a fornire una descrizione della tipologia di archivi adottati, inoltre dovrà controllare gli accessi e le tempistiche di aggiornamento dell'archivio stesso;

- La minimizzazione dei dati, tecnica che permette al titolare che avere a disposizione solo i dati necessari al raggiungimento delle finalità del trattamento. Essa può essere effettuata attraverso la rimozione di quei dati considerati superflui al trattamento, oppure riducendo l'accumulazione dei dati, oppure attraverso il filtraggio di essi.

Successivamente alla domanda numero otto viene chiesto al Titolare di elencare le misure applicate ai sistemi di sicurezza per garantire la protezione dei dati. Queste potrebbero essere:

- Misure riguardanti la gestione delle postazioni lavorative intente ad attenuare la possibilità di danneggiare i dati personali, danneggio che può avvenire grazie all'impiego di risorse aziendali disponibili, come i sistemi operativi, i software o le applicazioni aziendali;

- Ridurre il rischio di sfruttamento delle caratteristiche di un sito web per compromettere i dati personali, quindi misure che hanno la finalità di garantire la sicurezza dei siti web;

- Mettere in atto sistemi di protezione in base al tipo di rete impiegato volte alla sicurezza dei canali informatici, come ad esempio le sonde anti-intrusione;

- Mettere in atto misure utili per garantire la sicurezza dell'hardware, ovvero misure aventi lo scopo di attenuare il rischio che si incorre qualora l'utilizzo delle apparecchiature, come per esempio il computer portatile, viene impiegato per danneggiare i dati personali;

- Mettere in atto politiche di backup tese a garantire che il backup avvenga frequentemente;

- Mettere in atto una politica di manutenzione dei sistemi di sicurezza. La manutenzione può avvenire sia da remoto che fisicamente;

- Aumentare il controllo degli accessi fisici agli uffici trattamenti dati, ad esempio tramite l'adozione del badge;

- Mettere in atto misure che hanno l'obbiettivo di salvaguardare l'accesso a reti pubbliche o non controllate;

- Mettere in atto misure aventi la finalità di prevenire le fonti di rischio, che siano esse umane o non. Queste misure devono essere descritte minuziosamente durante il processo di DPIA;

- Adozione di una politica volta a porre dei limiti alla gravità e probabilità dei rischi per tutte le risorse impiegate nel trattamento dei dati. A tal fine si potrebbe documentare ciascuna procedura operativa, effettuare il duplicato dei dati trattati, limitare l'accesso ad essi, fare il backup con una certa frequenza, aggiornare i software, ecc.

Per quanto attiene il livello organizzativo, anche in questo campo vengono intraprese delle misure di sicurezza, che possono essere ad esempio:

- Adottare una politica di tutela della privacy che comprenda le linee guida e i controlli sull'attività di protezione dei dati;

- Informare tutti gli organi aziendali e i dipendenti dell'organizzazione sul comportamento da intraprendere dinnanzi a un trattamento dati; e provvedere alla formazione dei dipendenti in merito;

- Definire i processi di controllo e la gestione dei rischi;

- Definire un'organizzazione operativa che si occupi dell'individuazione e della gestione di tutti i fenomeni che possono incidere in maniera negativa sui diritti e sulle libertà delle persone;

- Inserire all'interno di ciascun progetto dell'organizzazione il concetto di protezione dei dati personali;

- Attuare delle misure di vigilanza sui dati, che possono essere sia di carattere materiale, come ad esempio la chiusura a chiave degli armadi in cui sono custoditi i dati o delle porte USB sui computer contenenti dati personali, che di conformità al Regolamento, ovvero effettuare delle periodiche verifiche in merito alla gestione dei trattamenti;

- Porre delle limitazioni in merito all'accesso da parte di terzi ai dati personali.

Per quanto riguarda le domande successive esse si concentrano sull'accesso illegittimo ai dati, sulle modifiche indesiderate ai dati ed infine la loro perdita. L'incaricato nel rispondere alle domande distribuisce una serie di elenchi in merito alle problematiche sopra citate. Il contenuto degli elenchi – che deve fornire una descrizione molto dettagliata – riguarda le minacce, le fonti di rischio, gli impatti e le misure di mitigazione del rischio.

Una volta conclusa questa parte si arriva alla penultima domanda, la quale pone l'attenzione sull'esistenza di un piano di intervento qualora si verifichi la *data breach*. Si

ricorda che la violazione dei dati comporta alla perdita dei dati, che può avvenire accidentalmente o in modo illegittimo, alla modifica, alla divulgazione a terzi non autorizzati, alla perdita del controllo dei dati personali, alla limitazione dei diritti degli interessati, alla discriminazione, al furto od usurpazione d'identità, alle perdite finanziarie, alla decifratura non autorizzata, ad un pregiudizio alla reputazione, ecc. (Considerando 85). Se si dovesse verificare la violazione dei dati, l'organizzazione deve aver precedentemente predisposto un piano di intervento al fine di evitare l'avanzamento dei danni fisici, materiali o immateriali agli interessati. Il piano di intervento è, per l'appunto, un piano che stabilisce le misure tecnologiche e organizzative idonee alla gestione della situazione, nonché la modalità con cui si deve intervenire. Oltre a questo, bisogna ricordare l'importanza di informare dell'accaduto l'Autorità di controllo entro e non oltre le 72 ore dal momento in cui il Titolare viene a conoscenza della violazione, o ad ogni modo senza ingiustificato ritardo. L'inosservanza di questa norma porta al peggioramento delle conseguenze sia per l'interessato che per il Titolare, il quale vede attaccata la propria reputazione oltre a dover pagare anche una sanzione amministrativa pecuniaria. Tuttavia, l'obbligatorietà della comunicazione decade se il Titolare è in grado di dimostrare che la violazione dei dati non è così grave da registrare un rischio per i diritti e le libertà della persona interessata o se è in grado di dimostrare che portare a conoscenza gli utenti della violazione comporti uno sforzo eccessivo. Oltre a comunicare la violazione all'Autorità Garante, il Titolare deve informare anche l'interessato, senza indebito ritardo. Il contenuto della comunicazione comprende una descrizione della natura della *data breach* e delle raccomandazioni tese ad attenuare i possibili effetti negativi. In questo caso non viene previsto un limite temporale entro il quale il titolare deve comunicare la violazione dei dati al soggetto interessato, tuttavia essa deve avvenire in tempi ragionevoli. Se però, la violazione dovesse essere comunicata in ritardo a causa dell'attuazione delle misure volte a contenderla, il Titolare sarebbe giustificato. Ad ogni modo, se il Titolare ha attuato tutte le misure utili per contrastare le conseguenza della violazione e dei relativi rischi decade l'obbligo di comunicare all'interessato in merito alla violazione dei dati.

Dunque, prendendo in considerazione quanto appena detto, il Titolare deve avere a disposizione un piano di gestione di questi eventi, nonché delle misure tecniche che lo aiutino ad individuare e successivamente comunicare la violazione dei dati. In altre parole, il piano di interventi deve contenere le seguenti informazioni:

- Come viene identificata la tipologia di rischio sotto esame? Una volta determinata la tipologia di rischio si ha la possibilità di intervenire. Ma per poter intervenire si devono avere presenti i seguenti parametri: la natura della violazione, il volume dei dati violati e del numero delle persone coinvolte;

- Le prime misure da intraprendere e a chi rivolgersi per mettersi in contatto con il

DPO e le società che gestiscono la tipologia dell'accadimento;

- Come viene valutata la probabilità concernente i rischi per i diritti e le libertà degli interessati conseguenti alla violazione?

- Qual è la procedura da seguire nel caso in cui si debba comunicare all'Autorità di controllo e alle persone interessate dell'avvenuta violazione?

Infine, l'ultima parte è dedicata all'opinione del Responsabile della Protezione dei Dati in merito alla Valutazione di impatto sulla protezione dei dati.

4.5.3 La Sintesi

Una volta che sono state fornite tutte le informazioni concernenti il trattamento al fine di avere un'analisi qualitativa-quantitativa dello stesso, si passa allo step successivo, ovvero al calcolo del rischio potenziale di ciascun elemento descritto nella colonna degli adempimenti. Il calcolo del rischio potenziale deve essere eseguito ancor prima di svolgere le varie attività di verifica. Il suo calcolo avviene attraverso l'impiego del modello adottato dall'organizzazione, ed è di fondamentale importanza, in quanto permette all'incaricato, insieme all'attività di controllo, di calcolare il rischio residuo.

Quello che deve fare l'incaricato è inserire all'interno della colonna dedicata al rischio potenziale il risultato conseguito sulla base dell'analisi del rischio potenziale di ciascun elemento della colonna dedicata agli adempimenti. Qualora uno degli elementi non fosse preso in considerazione dall'organizzazione, come valore si potrà inserire la dicitura "non applicabile". Sulla base del valore inserito, il sistema fornisce in modo automatico l'indice di rischio potenziale, che potrà risultare alto, medio, basso o non applicabile. In seguito, si passa alla fase di controllo su ciascun elemento, dopo di che nella colonna dedicata alla valutazione del presidio si inserisce il risultato della valutazione stessa. Tale risultato potrà essere (A)=adeguato, (IPA)=in prevalenza adeguato, (PA)=parzialmente adeguato, (IPI)=in prevalenza inadeguato, (IA)=inadeguato/assente, (NA)=non applicabile.

Per arrivare a determinare lo scoring di rischio, la check-list prima incrocia il valore del rischio potenziale e la valutazione del presidio ottenendo in modo automatico il rischio residuo, il quale successivamente viene tramutato nello scoring di rischio. Quest'ultimo può essere un numero intero compreso tra 0 e 5, escluso il 3. È molto importante il numero associato allo scoring in quanto rappresenta un giudizio secondo la seguente classifica:

- In corrispondenza del valore 5 il livello di rischio si considera di continuità;

- In corrispondenza di 4 il livello di rischio è elevato;

- In corrispondenza di 2 il livello di rischio risulta essere mediamente elevato;

- In corrispondenza del valore 1 il livello di rischio viene considerato mediamente basso;
- In corrispondenza di 0 il livello di rischio risulta basso.

Calcolato lo scoring di rischio per ciascun elemento, bisogna eseguire il calcolo dello scoring totale del trattamento. In merito si consideri la tabella all'interno del file denominato "sintesi". La tabella effettua in maniera automatica il calcolo dello scoring residuo medio, tenendo conto dei vari indici di rischi potenziali e degli scoring residui. Un esempio di questa tabella può essere il seguente:

Privacy					
DISTRIBUZIONE DEI RISCHI PER INDICE DI RISCHIO POTENZIALE E SCORING RESIDUO					
Scoring residuo	Indice di Rischio Potenziale				Totale Rischi
	Continuità	Alto	Medio	Basso	
5	0	0	0	0	0
4	0	7	0	0	7
2	0	5	2	0	7
1	0	7	2	0	9
0	0	2	0	0	2
Totale Rischi	0	21	4	0	25
SCORING RESIDUO MEDIO					
2,04	Mediamente elevato				

Figura 4.5: Calcolo dello scoring residuo medio in merito al trattamento dei dati nel settore bancario.

Anche in questo caso il valore dello scoring residuo medio oscilla tra lo 0 e il 5 e a seconda del valore ottenuto si hanno cinque giudizi differenti:

- Valore compreso tra 0 e 0,50, allora lo scoring medio può essere considerato basso;
- Valore all'interno dell'intervallo 0,50 e 1,50, lo scoring medio risulta mediamente basso;
- Valore tra 1,50 e 3, allora lo scoring medio è mediamente elevato;
- Valore tra 3 e 4,50, lo scoring medio è considerato elevato; - Valore maggiore di 4,50, lo scoring medio risulta in continuità.

4.5.4 Il Masterplan degli interventi

Il Masterplan degli interventi costituisce l'ultima sezione del modello di DPIA. Questa parte è molto utile durante la fase del monitoraggio e riesame della DPIA, che come è

stato detto più volte, è un processo dinamico, il che implica un monitoraggio continuo. Il Masterplan degli interventi è costituito da una serie di colonne che in parte riprendono quelle precedentemente approfondite nel file denominato "check-list" come "gli adempimenti", "l'indice di rischio residuo" e "le criticità" individuate in fase di verifica. Proseguendo, alla quarta colonna si trovano "gli interventi" che il Titolare dovrà mettere in atto a seconda delle criticità riscontrate e delle scoring di rischio ottenuto, al fine di attenuare il rischio, quindi ottenendo un valore migliore.

Anche la quinta colonna riguardante la "Documentazione organizzativa da implementare" ha l'obiettivo di raccogliere le necessità che si riscontrano di implementare della documentazione aggiuntiva rispetto a quella attualmente adottata. Infine, l'ultima colonna, concernente la "Tempistica", indica il tempo entro cui dovranno vedersi compiute le attività e la documentazione aggiuntiva richiesta dal Titolare al fine di riuscire a portare a termine il trattamento in conformità del Regolamento.

4.6 Applicazione del Modello di DPIA

Fin ora è stato descritto un modello di Valutazione d'impatto e il suo funzionamento senza però applicarlo in 'uno specifico scenario. Tant'è vero che si è sempre parlato di un'organizzazione generica senza specificare l'attività di essa e la tipologia di dati trattati. Di seguito si studierà l'applicazione del modello in cinque realtà diverse tra di loro:

1. La videosorveglianza sul posto di lavoro;
2. I dati medici in azienda ospedaliera;
3. La richiesta del casellario giudiziario a fini assuntivi;
4. Telemarketing e l'accesso a banche dati;
5. Trattamento dei dati nel settore bancario.

Prima di procedere con l'analisi dei cinque scenari, bisogna fare una piccola introduzione al modello utilizzato per l'identificazione, la valutazione e la gestione dei rischi, sia di quelli quantificabili che non, ovvero il CoSo Report. Il CoSo Report (Committee of Sponsoring Organizations of the Treadway Commission) fu sviluppato nel 1992 da una Commissione statunitense indipendente sovvenzionata dalle maggiori associazioni professionali-industriali dello Stato. Questo modello gioca un ruolo fondamentale all'interno dell'organizzazione, in quanto mette a disposizione delle linee guida per la gestione degli eventi incerti che possono verificarsi, nonché per la determinazione del livello di rischio accettabile in relazione agli obbiettivi prefissati. Esso viene considerato il precursore di un

modello attuale e di una certa notorietà impiegato nella gestione dei rischi, ossia *l'Enterprise Risk Management*[21] sviluppato nel 2004. Ritornando al modello CoSo Report, solitamente viene attuato dall'*Internal Audit*, funzione che si occupa della determinazione delle criticità tipiche di ciascun processo dell'organizzazione, nonché della stima dei potenziali rischi, durante quest'ultima fase l'*Internal Audit* collabora con il *Risk Management*. In primis, nell'attuazione del modello, bisogna comprendere l'esistenza di fattori che comportino impatti negativi sul trattamento, ovvero causare danni ai diritti e alle libertà della persona in merito ai dati personali. Tale impatto viene specificato attraverso due passi consecutivi: il primo prevede la misurazione del rischio attinente e il secondo – la misurazione del rischio residuo. Per quanto riguarda il rischio[22] inerente, è quel rischio iniziale al quale l'organizzazione è soggetta in mancanza dell'adozione delle misure di sicurezza volte ad attenuarlo. La sua misurazione avviene considerando due variabili, ossia la probabilità[23] del verificarsi del fenomeno negativo e l'impatto[24] che esso avrebbe sul trattamento. Invece con l'espressione "rischio residuo" si intende il rischio che permane in seguito all'attuazione delle misure di sicurezza volte all'attenuazione del rischio stesso da parte dell'organizzazione.

In questa sede non si effettuerà la valutazione del rischio, bensì la Valutazione d'impatto sulla protezione dei dati (DPIA), tema su cui converte l'intero elaborato. Come già presentato nel dettaglio il modello di DPIA e accennato la sua applicazione all'interno di cinque realtà diverse, si vuole riprendere dall'applicazione del modello nell'ambito della videosorveglianza sul posto di lavoro.

4.6.1 La videosorveglianza sul posto di lavoro

Prima di passare alla Check-list bisogna precisare perché la videosorveglianza sul posto di lavoro è considerata trattamento di dati personali e per questo motivo sottoposto alla valutazione d'impatto sulla protezione dei dati. La videosorveglianza rappresenta un tipo di tecnologia caratterizzata dalla possibilità di controllare a distanza[25] le persone. Le immagini, in caso di videosorveglianza, qualora si riferiscono a persone fisiche, implicano un trattamento di dati personali. Di conseguenza, il Titolare del trattamento deve rispettare

[21] "L'ERM è un processo, gestito dal CdA della banca, dal management e dal personale; utilizzato per la formulazione di strategie in tutta l'organizzazione; progettato per identificare gli eventi potenziali che possono influire sull'attività aziendale, per gestire il rischio entro i limiti tollerati al fine di fornire una ragionevole assicurazione che gli obiettivi dell'organizzazione vengano raggiunti."

[22] In merito alla definizione del concetto di rischio in materia di dati personali si veda il Considerando 75 – GDPR.

[23] Per "probabilità" si intende il rapporto tra occasioni in cui il rischio si è trasformato in vero e proprio danno e il numero totale dei rischi.

[24] Per "impatto" si intende l'effetto sui diritti personali o sui diritti patrimoniali coinvolti. In termini economici rappresenta una spesa sostenuta nell'intento di recuperare la situazione antecedente al verificarsi del fenomeno e di risarcimento della persona danneggiata.

[25] Con l'espressione "controllo a distanza" si intende una particolare tipologia di controlli datoriali caratterizzati dall'utilizzo di apparecchiature e denominati per questo motivo "controlli tecnologici".

le disposizioni di legge previste dal Regolamento UE n. 2016/679, oltre che la normativa nazionale, in special modo l'articolo 114, il quale rimanda all'articolo 4 della legge 20 maggio 1970, n. 300, ovvero lo Statuto dei Lavoratori, come modificato dal D. Lgs. n. 151/2015 (la cosiddetta *Jobs Act*).

Dunque in questo caso risulta di fondamentale importanza l'articolo 4 dello Statuto dei lavoratori, per questo motivo si è preferito riportarlo di seguito:
"Art. 4 - Impianti audiovisivi.

1. Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione delle sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.

2. La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

3. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196."

Analizzando i vari commi si può affermare quanto segue: al comma 1 viene sancito che gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere utilizzati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Inoltre, l'installazione di queste apparecchiature deve avvenire previo accordo sindacale o, se esso dovesse mancare, previa autorizzazione dell'Ispettorato Nazionale del Lavoro. Successivamente, al comma 2 viene stabilita la non applicabilità del comma 1 agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione e degli accessi e delle presenze. Questi ultimi strumenti permettono di

tener traccia non solo delle entrate e delle uscite nella/dalla sede aziendale, ma anche degli eventuali spostamenti da una filiale all'altra ad esempio. Infine, il comma 3 prevede che l'utilizzo delle informazioni raccolte ai fini connessi al rapporto di lavoro è ammesso purché il lavoratore sia stato informato in merito alla modalità di utilizzo degli strumenti di controllo a distanza e vengano rispettate le disposizioni previste nel Codice della Privacy.

In merito, si tiene a precisare che il divieto di controlli a distanza sull'operato del lavoratore si riferisce in via esclusiva all'utilizzo di apparecchiature di controllo. Tale chiarimento costituisce un punto di notevole importanza, in quanto controlli diretti da parte del datore di lavoro o svolti attraverso un suo incaricato non rientrano nell'ambito di applicazione dell'articolo 4, che, essendo sanzionato penalmente, non ammette interpretazioni analogiche.

Un altro punto che necessita di un chiarimento riguarda l'installazione della apparecchiature, ma non il loro funzionamento. In merito, bisogna ritornare sul concetto di "distanza", esso si riferisce sia alla distanza fisica, sia quella temporale. Di conseguenza, i fenomeni quali il mancato funzionamento dell'apparecchiatura, la consapevolezza della sua presenza da parte dei dipendenti o il suo utilizzo discontinuo ai fini di controllo non sono esclusi dal divieto di controllo a distanza previsto all'articolo 4 dello Statuto dei lavoratori.

Infine, i datori di lavoro devono tener conto del Provvedimento generale in tema di videosorveglianza del 8 aprile 2010, il quale anche in seguito all'emanazione del Regolamento generale sulla protezione dei dati continua ad applicarsi con i dovuti adattamenti. Il Provvedimento ha natura descrittiva in quanto fu emanato ai sensi dell'articolo 154, comma 1, lett. c) del vecchio Codice della Privacy. Ne seguiva che la sua violazione era sottoposta al dettato normativo dell'articolo 162, comma 2-ter del Codice della Privacy, ossia: *"In caso di inosservanza dei provvedimenti di prescrizione di misure necessarie o di divieto di cui, rispettivamente, all'art. 154, comma 1, lett. c) e d), è altresì applicata in sede amministrativa, in ogni caso, la sanzione del pagamento di una somma da trentamila euro a centottantamila euro".*

Inoltre, per quanto concerne i sistemi di videosorveglianza installati senza accordo o autorizzazione da parte dell'INL (comprese le telecamere finte) il Ministero del Lavoro e delle Politiche Sociali in data 1 giugno 2016 ha espresso un parere precisando gli aspetti sanzionatori e gli accertamenti ispettivi, riconfermando il divieto imposto dall'articolo 4 legge n.300/1970.[26]

[26]Legge n.300/1970 modificata successivamente al Parere espresso dal Ministero del Lavoro e delle Politiche sociali dal D. Lgs. 24 settembre 2016, n.185.

Una volta chiariti questi punti si può passare alla Valutazione d'impatto sulla protezione dei dati, iniziando dalla prima sezione, ovvero la Check-list. Per quanto riguardano le colonne dedicate agli adempimenti, ai riferimenti normativi e alle attività di verifica non viene registrato alcun cambiamento rispetto al modello generale. La componente che invece varia a seconda della tipologia di trattamento analizzato è il Rischio residuo, ovvero la parte di rischio che permane in seguito all'adozione delle misure di mitigazione del rischio potenziale relativo a ciascun elemento. In merito, si consulti la Check-list relativa alla videosorveglianza sul posto di lavoro in allegato "Capitolo 5."

Ed inoltre si riporta la tabella all'interno del file denominato "sintesi", la quale – come detto precedentemente – calcola automaticamente lo scoring residuo medio tenendo conto dei vari indici di rischi potenziali e degli scoring residui.

Privacy					
DISTRIBUZIONE DEI RISCHI PER INDICE DI RISCHIO POTENZIALE E SCORING RESIDUO					
Scoring residuo	Indice di Rischio Potenziale				Totale Rischi
	Continuità	Alto	Medio	Basso	
5	0	0	0	0	0
4	0	6	0	0	6
2	0	7	3	0	10
1	0	4	0	0	4
0	0	2	0	0	2
Totale Rischi	0	19	3	0	22
SCORING RESIDUO MEDIO					
2,26	Mediamente elevato				

Figura 4.6: *Calcolo dello scoring residuo medio in merito alla videosorveglianza sul posto di lavoro.*

Come si può osservare dalla *Figura 4.6*, lo scoring residuo medio risulta mediamente elevato, in quanto il valore risultante è 2,26.

4.6.2 I dati medici in azienda ospedaliera

Il trattamento dei dati relativi alla salute è vietato dall'articolo 9 del Regolamento generale sulla protezione dei dati, in quanto i dati relativi alla salute fanno parte della categoria dei dati sensibili. I dati sensibili riguardano informazioni concernenti gli aspetti più intimi della vita di un individuo e sono tassativamente indicati dalla norma. Data l'importanza dei dati sensibili, si riporta la norma che ne vieta il loro trattamento, l'articolo 9, comma 1 recita: *"È vietato trattare 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."

Per quanto attiene i dati relativi alla salute, il RGPD li definisce all'articolo 4, num. 15), come *"i 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."*

In merito il considerando 35 chiarisce che: *"Nei dati personali relativi alla salute dovrebbero rientrare tutti i dati riguardanti lo stato di salute dell'interessato che rivelino informazioni connesse allo stato di salute fisica o mentale passata, presente o futura dello stesso. Questi comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria o della relativa prestazione di cui alla direttiva 2011/24/UE del Parlamento europeo e del Consiglio (9); un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari; le informazioni risultanti da esami e controlli effettuati su una parte del corpo o una sostanza organica, compresi i dati genetici e i campioni biologici; e qualsiasi informazione riguardante, ad esempio, una malattia, una disabilità, il rischio di malattie, l'anamnesi medica, i trattamenti clinici o lo stato fisiologico o biomedico dell'interessato, indipendentemente dalla fonte, quale, ad esempio, un medico o altro operatore sanitario, un ospedale, un dispositivo medico o un test diagnostico in vitro."*

Un'altra specificazione che bisogna fare in merito ai dati sanitari, essi vengono classificati dalla normativa europea come dati sensibili, tuttavia la Cassazione nazionale considera i dati relativi alla salute insieme ai dati relativi alla vita sessuale delle persone dati "supersensibili",[27] perché riguardano la parte più intima dell'individuo, di conseguenza necessitano di una tutela rafforzata.

Ritornando alla normativa europea, l'articolo 9 impone il divieto di trattare tale categoria di dati, tuttavia il divieto decade se persistono una serie di circostanze, ad esempio nel settore sanitario le circostanze sono riconducibili all'erogazione della prestazione stessa. Vi sono altre situazioni che legittimano il trattamento dei dati sanitari, ad esempio la necessità del trattamento per finalità di medicina preventiva, o di medicina del lavoro. Il medico del lavoro valuta la capacità lavorativa del dipendente, senza però svelare al datore di lavoro la patologia riscontrata nel paziente, – in questo caso il dipendente – ma si limita a certificare l'idoneità del lavoratore a svolgere quel determinato lavoro.

[27] Cassazione, sezione VI, sentenza del 11 gennaio 2016, n. 222; sezione I, sentenza del 7 ottobre 2014, n. 21107; sezione I, sentenza del 1 agosto 2013, n. 18443.

Ovviamente queste circostanze sono oltre alle circostanze tradizionali in cui il trattamento è necessario per motivi di interesse pubblico nel settore della pubblica sanità, come ad esempio la protezione da gravi minacce per la salute pubblica. Dunque, secondo l'ottica del GDPR bisogna perseguire l'interesse pubblico nel settore della sanità e questo funge da giustificazione dell'inosservanza del divieto di cui all'articolo 9, comma 1.

Di notevole importanza è l'informativa e il consenso in virtù del principio di trasparenza previsto dal GDPR. Come è già stato detto più volte, il titolare deve provvedere a comunicare all'interessato tutte le informazioni riguardanti il trattamento dei dati personali, e tali informazioni devono essere secondo l'articolo 12: *"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, se del caso in formato elettronico. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato."*

Per quanto concerne il consenso, questo deve essere, ai sensi dell'articolo 7, informato, specifico e che venga prestato dall'interessato in piena libertà. Inoltre, il GDPR impone che il consenso avvenga tramite un atto affermativo e chiaro da parte del soggetto interessato. In particolare nell'ambito sanitario non ci deve essere ambiguità in merito l'intenzione del paziente di rendere i propri dati sanitari oggetto di un trattamento. Ad esempio il silenzio-assenso dell'interessato o la predisposizione da parte del titolare o del responsabile del trattamento di caselle preselezionate non possono essere considerate forme di consenso conforme al Regolamento UE n. 2016/679. Sempre in merito alla tematica del consenso tratta anche l'articolo 8, che detta particolari condizioni nell'interesse dei minori, il quale specifica che il trattamento di dati personali di minori al di sotto dei 16 anni, o se previsto da diritto degli Stati membri, di un'età inferiore (max. 13 anni), è lecito se vi è il consenso espresso e autorizzato dai genitori o dal tutore del minore.

Un'altra tematica che merita una breve discussione è il trattamento automatizzato dei dati personali che possano sfociare in decisioni automatizzate, inclusa la profilazione, con conseguenti effetti giuridici sull'interessato. In merito, l'articolo 22, riconosce il diritto in capo all'interessato di non essere sottoposto ad un processo decisionale automatizzato, quindi vieta tale processo, tranne quando vi è la necessità di concludere un contratto tra l'interessato e il titolare o, quando il processo decisionale automatizzato è autorizzato dal diritto UE o dal diritto degli Stati membri a cui è soggetto il titolare, e che venga garantito lo stesso livello di sicurezza per i diritti e le libertà degli individui o, se vi è l'esplicito consenso da parte dell'interessato.

Un ultimo punto da considerare è la cosiddetta sanità elettronica o digitale. Grazie allo sviluppo tecnologico, nell'ambito della sanità vengono introdotti nuovi strumenti rivoluzionari, quali il Fascicolo Sanitario Elettronico (FSE), il Dossier sanitario, i referti online, la ricetta elettronica, le prenotazioni sanitarie online, i certificati di malattia telematici, ecc. Tuttavia, se da una parte l'avanzare della tecnologia comporta dei notevoli vantaggi in termini di riduzione delle tempistiche, di semplificazione dell'operazione di rintracciare e dello scambio di informazioni tra operatori e utenti, dall'altra comporta anche un aumento del volume di dati personali trasmessi e trattati il che implica l'aumento anche del rischio connesso al loro utilizzo da parte di terzi non autorizzati. In risposta a questo problema il Regolamento generale sulla protezione dei dati tende ad instaurare un quadro giuridico solido e coerente in materia di protezione dei dati nell'UE, grazie all'adozione di misure efficaci, contribuirà anche allo sviluppo dell'economia digitale nel mercato interno, oltre a garantire alle persone fisiche il controllo dei loro dati personali. In particolare nel settore della sanità digitale troveranno applicazione i principi previsti dal GDPR, come il già discusso principio dell'*accountability* – vero e proprio pilastro su cui si basa il Regolamento – il principio della trasparenza, il principio della *Privacy by Design* e *by Default*, nonché gli obblighi in capo al Titolare e al Responsabile del trattamento, come il Registro delle attività di trattamento, la Valutazione di impatto sulla protezione dei dati (DPIA) e la violazione dei dati.

Una volta effettuato questa introduzione al trattamento in ambito sanitario, si passa al passaggio successivo, ovvero all'applicazione del modello di DPIA nell'azienda ospedaliera. Al riguardo si consulti il file denominato "Check-list privacy – Ospedale" presente in allegato al capitolo 5.

Per quanto concerne lo scoring residuo medio si può affermare che questo è decisamente basso, ovvero 1.43, valore classificato come mediamente basso, come calcolato nella tabella seguente:

Privacy					
DISTRIBUZIONE DEI RISCHI PER INDICE DI RISCHIO POTENZIALE E SCORING RESIDUO					
Scoring residuo	Indice di Rischio Potenziale				Totale Rischi
	Continuità	Alto	Medio	Basso	
5	0	0	0	0	0
4	0	2	0	0	2
2	0	3	1	0	4
1	0	9	3	0	12
0	0	2	0	0	2
Totale Rischi	0	16	4	0	20
SCORING RESIDUO MEDIO					
1,43	Mediamente basso				

Figura 4.7: *Calcolo dello scoring residuo medio concernente il trattamento dei dati personali in ambito della sanità.*

4.6.3 Richiesta del Casellario Giudiziario a fini assuntivi

Il certificato di Casellario giudiziario o – come si usa dire nel linguaggio comune – la fedina penale, nell'ordinamento giuridico italiano, è un certificato che viene istituito su richiesta dell'interessato presso la Procura della Repubblica di ogni tribunale ordinario della Repubblica italiana, il cui contenuto riguarda i precedenti penali e civili del richiedente.

Spesso, in sede di assunzione il datore di lavoro chiede il certificato del Casellario giudiziario al futuro dipendente per assicurarsi che egli non abbia commesso reati.

Ma nell'ottica del Regolamento UE questa prassi non è permessa. Infatti l'articolo 10 tratta i dati personali relativi a condanne penali e reati, stabilendo che: *"Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica."* Dunque l'articolo 10 sancisce la liceità del trattamento dei dati giudiziari, il quale, oltre a soddisfare le condizioni di liceità previste all'articolo 6, paragrafo 1, deve soddisfare ulteriori 2 condizioni, ovvero:

1. Il controllo dell'Autorità pubblica;

2. L'autorizzazione specifica basata sul diritto dell'UE o dello Stato membro che preveda garanzie appropriate per i diritti e le libertà degli interessati.

In contemporanea all'articolo 10 va considerato l'articolo 2-octies del Codice della Privacy come modificato dal D. Lgs. 101/2018 recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679. L'articolo 2-octies – tenuto conto del D. Lgs. 51/2018 recante l'attuazione della Direttiva UE 2016/680[28] - stabilisce che qualora il trattamento di dati relativi a condanne penali e a reati non sia soggetto al controllo dell'Autorità pubblica, esso è consentito, sulla base dell'articolo 10 del GDPR, solo se autorizzato da una norma di legge o di regolamento, che prevedano una tutela appropriata per i diritti e le libertà degli interessati. Al comma 2 del suddetto articolo, viene precisato il fatto che *"in mancanza delle predette disposizioni di legge o di regolamento, i trattamenti dei dati di cui al comma 1 nonché le garanzie di cui al medesimo comma sono individuate con decreto del Ministro della giustizia, da adottarsi, ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, sentito il Garante."*

Puntualizzato il quadro normativo di riferimento, si può esprimere con certezza che in fase di assunzione il datore di lavoro non può chiedere al candidato il certificato di Casellario giudiziale, dal momento che manca un'autorizzazione legale di questo genere e questo implica l'illiceità del trattamento, di conseguenza il datore di lavoro non può trattare i dati relativi alle condanne penali e ai reati, anche in presenza del consenso del candidato. Sul ultimo punto si tiene a precisare che nonostante ci sia il consenso espresso in modo esplicito da parte dell'interessato, il Regolamento generale sulla protezione dei dati vieta il trattamento dei dati giudiziari. In merito all'autorizzazione, ad esempio se si fa riferimento all'assunzione nel settore dell'industria finanziaria, la richiesta del certificato di Casellario giudiziale può avvenire, in base al articolo 2-octies del Codice della Privacy, solo se autorizzato da una norma di legge, che nel caso del settore bancario è il Contratto Nazionale ABI (Associazione Bancaria Italiana) e nel settore assicurativo il Contratto Assicurativo ANIA (Associazione Nazionale fra le Imprese Assicurative). Nessuno dei due contratti prevede il trattamento dei dati giudiziari, di conseguenza non compare da nessuna parte la richiesta dell'utilizzo de Casellario giudiziale ai fini assuntivi.

Qualora il datore di lavoro, in violazione della normativa europea, chiedesse il Casellario giudiziale, egli incorre nelle sanzioni pecuniarie previste dal GDPR che possono giungere fino a 20 milioni di euro o al 4 percento del fatturato se superiore.

[28] 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.

4.6.4 Telemarketing e l'accesso a banche dati

Il telemarketing consiste nel contatto, tramite l'impiego del telefono e con l'ausilio di un operatore (call-center), tra l'azienda e la sua clientela, ai fini di invio di materiale pubblicitario o di vendita diretta o di ricerche di mercato o di comunicazione promozionale.[29]

Definito il concetto di telemarketing, si vuole porre l'attenzione sul telemarketing aggressivo o selvaggio, ovvero quel fenomeno a cui tutti i cittadini devono subire, spesso anche più volte durante il corso della giornata, ovvero le chiamate indesiderate da parte dei call center. Questi ultimi, pur di vendere il prodotto o il servizio, chiamano nei momenti meno opportuni, disturbando continuamente, perché il più delle volte propongono prodotti o servizi non compatibili con i reali bisogni e gusti della persona contattata. Le domande che sorgono spontanee sono: da dove prendono i recapiti telefonici? Hanno il consenso dell'interessato al trattamento dei dati personali? I dati di contatto si possono trovare negli elenchi telefonici pubblici, o acquistando banche dati da società terze (le cosiddette *cold list*), o sul web attraverso la compilazione di un forum di contatto, oppure nel corso di eventi organizzati ecc. In merito al consenso, molto spesso il consenso al telemarketing viene dato inconsapevolmente, o che sia per non aver letto il contenuto riguardante il consenso al trattamento dei propri dati, che fra l'altro è sempre scritto con caratteri molto piccoli, aver firmato una sola volta questi testi minuscoli è sufficiente per perdere il controllo sui propri dati. Ed è proprio in questo modo che il numero di cellulare entra nel mercato della rivendita a terzi, da qui le innumerevoli segnalazioni concernenti le chiamate pubblicitarie non autorizzate al Garante Privacy.

In passato l'attività di telemarketing è stata oggetto di normative e tutele particolari si da parte dell'Autorità garante per le comunicazioni (AGCOM) sia dal Garante Privacy. In merito, ci sono due provvedimenti da parte dell'Autorità Garante Privacy nazionale risalenti rispettivamente nel 2003 e nel 2013. Il provvedimento generale del 29 maggio 2003 "Regole per un corretto uso dei sistemi automatizzati e l'invio di comunicazioni elettroniche" stabilisce dei confini nell'utilizzo dei sistemi automatizzati e nell'invio di comunicazioni elettroniche. Dieci anni dopo vengono pubblicate le "Linee guida in materia di attività promozionale e contrasto allo spam".

Oggigiorno nel settore del telemarketing vige sia il GDPR sia la legge 11 gennaio 2018, n. 5, recante disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato, entrata in vigore il 4 febbraio 2018. La legge in questione funge da

[29] Definizione di telemarketing secondo M. SOFFIENTINI in *"Privacy-Protezione e trattamento dei dati"*, Assago, Ipsoa, 2018.

una tutela in più per gli utenti invasi dal telemarketing aggressivo grazie all'introduzione delle seguenti novità:

- Viene rafforzato il Registro Pubblico delle Opposizioni (attivato già dal 2011, che permette l'esercizio del diritto di opposizione dell'utente). Il contenuto di questo registro è costituito da un elenco di numeri a cui è vietato telefonare a fini commerciali, inclusi i numeri riservati, ovvero quelli assenti nell'elenco telefonico, nonché quelli di cellulare;

- Vengono annullati tutti i consensi dati dall'utente precedentemente all'iscrizione al registro delle opposizioni;

- Gli operatori dei call center devono comunicare all'utente la modalità con cui hanno ottenuto i suoi dati personali (la fonte, che può essere l'acquisto di banche dati da società terzi, o gli elenchi pubblici);

- Gli operatori dei call center devono effettuare le chiamate utilizzando i due prefissi individuati dalla AGCOM, ovvero il prefisso 0843 per le indagini statistiche e il prefisso 0844 per le ricerche di mercato e per le attività di pubblicità, vendita e comunicazione commerciale. Questo esclude l'utilizzo dei prefissi 02 o 06 o addirittura della propria città.

- Vengono vietate le chiamate casuali con sistemi automatici di composizione.

Anche precedentemente all'entrata in vigore della legge n. 5/2018 era vietato ai call center di chiamare i numeri riservati di cellulare in assenza di consenso dell'utente. Tuttavia, come accennato prima, il consenso concesso distrattamente da parte dell'utente implicava la possibilità di ricevere telefonate da parte degli operatori dei call center. In seguito all'entrata in vigore della suddetta legge, che permette di cancellare tutti i consensi concessi in precedenza una volta iscritto il proprio numero nel registro delle opposizioni, gli utenti godono di una maggiore tutela in merito, in quanto prima era molto difficile, se non addirittura impossibile, riuscire a negare il consenso concesso. La legge permette tuttavia un'eccezione: *"Sono fatti salvi i consensi prestati nell'ambito di specifici rapporti contrattuali in essere, ovvero cessati da non più di trenta giorni, aventi ad oggetto la fornitura di beni o servizi."* Questo significa che anche se è stato iscritto al registro il proprio numero telefonico, le società con cui si hanno in essere un contratto o quelle alle quali è stata fatta presente la disdetta da non più di 30 giorni, possono contattare l'utente. Quest'ultimo comunque ha la facoltà di revocare il consenso con modalità semplificate, che potrebbe essere ad esempio l'invio di una mail al proprio operatore telefonico.

Se ad ogni modo si dovessero continuare a ricevere chiamate di telemarketing, nonostante l'iscrizione del numero nel registro delle opposizioni e la revoca del consenso, l'utente

può avvalersi della facoltà di segnalare l'accaduto all'Autorità Garante. Il Garante provvederà a sanzionare la società di call center con sanzioni pecuniarie che possono arrivare fino al 4 percento del loro fatturato annuo, in quanto il trattamento dei dati personali risulta illecito dal momento che manca il consenso dell'interessato. In più c'è da dire che la nuova norma rende corresponsabili i soggetti che beneficiano della campagna di marketing, questo significa che il Garante può sanzionare non solo le società di call center ma anche gli stessi operatori telefonici che vi hanno ricorso. Tale disposizione funge da incentivo di investire in quelle società che adoperano in conformità delle disposizioni di legge.

Per essere conforme al GDPR e alla legge n. 5/2018 bisogna innanzitutto individuare la base giuridica per il legittimo trattamento per finalità di marketing. Ai sensi dell'articolo 6, paragrafo 1, lett. a) del GDPR il trattamento dei dati è lecito se l'interessato ha espresso il suo consenso, ed inoltre l'articolo 13 stabilisce che per essere considerato valido ed efficace deve essere stato concesso liberamente, in modo specifico ed in forma espressa in seguito ad un'informativa completa. Ecco il motivo per cui tutto ruota intorno al consenso, in special modo nel settore del telemarketing.

Inoltre, in questo settore risulta di fondamentale importanza la modalità con cui vengono raccolti i dati personali, che principalmente può avvenire o in modo diretto, ovvero l'imprenditore stesso raccoglie i dati presso l'interessato, al quale viene fornita in via preventiva un'informativa chiara e dettagliata in merito al loro utilizzo, in seguito raccolto il consenso al trattamento dei dati per finalità di marketing. Un'altra modalità con cui avviene la raccolta dei dati è la cosiddetta *cold list* (come accennato in precedenza), ovvero l'acquisto di banche dati da società terze. In questo caso entra in gioco il principio della responsabilizzazione, in base al quale il titolare del trattamento risulta, in via preliminare, il responsabile del trattamento, e per questo motivo deve essere in grado a dimostrare di aver adottato tutte le misure tecniche e organizzative per salvaguardare i diritti e le libertà fondamentali degli interessati e per poter dimostrare di aver agito conformemente al GDPR (art. 24). Alla luce di quanto detto, quando il titolare del trattamento raccoglie i dati personali tramite una società terza, egli deve chiedere alla società terza il rilascio di una dichiarazione in cui viene specificato che il consenso degli interessati è stato prestato in modo legittimo, ovvero secondo quanto previsto dal GDPR, ed inoltre deve chiedere una campionatura dell'informativa e del consenso.

Infine, vi è la modalità di acquisizione dei dati di contatto da elenchi o registri pubblici. In questo caso non è richiesto il consenso al trattamento dei dati degli interessati, e questa costituisce un'eccezione prevista nel Codice della Privacy all'articolo 130, comma 3-bis, fermo restando che l'interessato contattato non abbia esercitato il diritto di opposizione mediante l'iscrizione della propria numerazione nell'apposito registro delle opposizioni. Ad

ogni modo l'interessato nel momento della chiamata può chiedere di non essere più contattato per finalità di marketing, avvalendosi in questo modo dell'opzione *opt-out*, dopo che l'operatore del call center abbia reso l'informativa durante la chiamata. L'informativa potrà essere anche breve, purché l'operatore indichi il sito web contenente l'informativa completa. In altre parole, la telefonata da parte dell'operatore deve seguire il seguente iter:

- Presentazione dell'operatore;
- Indicazione dello scopo della chiamata e per conto di chi la effettua;
- Indicazione della fonte da dove sono stati prelevati i dati dell'utente;
- Rendimento dell'informativa (art. 13-GDPR);
- Indicazione della facoltà in capo all'interessato di esercitare il suo diritto di opposizione, nonché la possibilità di iscriversi all'apposito registro.

Un altro punto fondamentale gioca il controllo del Registro delle opposizioni prima di effettuare la telefonata a fini di marketing. Perché, se l'utente, che si voleva contare risultasse iscritto a tale registro, non potrà essere contattato.

Chiariti questi punti si può procedere con la Valutazione d'impatto sulla protezione dei dati, la quale viene riportata in allegato al capitolo 5.
Seguendo i vari step del modello di DPIA, ovvero l'analisi quantitativa-qualitativa del trattamento dei dati personali, il calcolo del rischio potenziale per ciascun adempimento, l'attività di verifica, il calcolo del rischio residuo, la trasformazione del rischio residuo in scoring di rischio per ciascun elemento, si arriva a determinare lo scoring residuo medio.

Privacy					
DISTRIBUZIONE DEI RISCHI PER INDICE DI RISCHIO POTENZIALE E SCORING RESIDUO					
Scoring residuo	Indice di Rischio Potenziale				Totale Rischi
	Continuità	Alto	Medio	Basso	
5	0	0	0	0	**0**
4	0	12	0	0	**12**
2	0	7	4	0	**11**
1	0	1	0	0	**1**
0	0	0	0	0	**0**
Totale Rischi	**0**	**20**	**4**	**0**	**24**
SCORING RESIDUO MEDIO					
3,00	Elevato				

Figura 4.8: *Calcolo dello scoring residuo medio concernente il trattamento dei dati personali nel settore del telemarketing.*

Come si evince dalla *Figura 4.8*, questo settore registra uno scoring residuo medio elevato.

4.6.5 Il trattamento dei dati personali nel settore bancario

Anche il settore bancario è sottoposto agli adempimenti previsti dalla normativa europea in materia di privacy e per di più si può affermare che gli istituti creditizi sono considerati i soggetti maggiormente colpiti dalle novità introdotte del GDPR, in quanto trattano una grande quantità di dati personali dei propri clienti. Questo implica oltre ai rischi inerenti il trattamento dei dati anche il rischio reputazionale, al quale si incorre anche qualora non si è conformi alle disposizioni del Regolamento generale sulla protezione dei dati.

Per evitare di essere sanzionate da parte dell'Autorità di controllo, le banche devono introdurre una serie di cambiamenti sia sul piano organizzativo che sul piano tecnico, come ad esempio:

- Aggiungere un ufficio dedicato alla protezione dei dati, data l'introduzione della figura del DPO all'interno della compagine sociale;

- Rivedere le figure Privacy ed implementare un modello operativo di governance per la protezione dei dati;

- Implementare processi di sviluppo e pianificazione dei trattamenti al fine di identificare i dati necessari al trattamento;

- Definire la base giuridica del trattamento (nel caso fosse il consenso, bisogna gestire in maniera consona l'acquisizione del consenso, predisponendo all'interessato l'informativa, assicurando l'esercizio dei diritti dell'interessato, ecc.);

- Formare il personale in materia di protezione dei dati;

- Rivedere la documentazione privacy, e se necessario apportare le integrazioni richieste dal GDPR, come la tenuta del Registro dei trattamenti;

- Provvedere all'aggiornamento, e se necessario anche al cambiamento, dell'infrastruttura e architettura IT;

- Ampliare la gestione dei metadata;

Tutte queste misure servono nella mitigazione dei vari rischi che gravano sulla Banca in quanto titolare del trattamento dei dati nonché nella salvaguardia dei diritti e delle libertà degli interessati. Tuttavia non sempre queste misure riescono nel loro obbiettivo. Il motivo risiede nella Direttiva UE 2015/2366 relativa ai servizi di pagamento nel mercato interno, che ha concesso a operatori, anche diversi dagli istituti creditizi – titolari del trattamento dei dati personali concernenti i propri clienti – di rendere tali dati di dominio pubblico, facilmente accessibili perseguendo lo scopo di creare un "mercato aperto ed equo".[30]

Quindi le Banche, in quanto titolari del trattamento dei dati dei propri clienti esercitano una bassa percentuale di controllo su tali dati, rincorrendo a diversi rischi, i quali:

- L'utilizzo delle informazioni del cliente da parte di terzi per acquisti abusivi, non autorizzati;

- Vengono violate da parte di terzi le condizioni per le quali il cliente aveva concesso il consenso alla Banca per il trattamento dei propri dati;

- L'utilizzo degli hacker da parte di terzi per aggirare i sistemi di controllo e cybersecurity dell'istituto creditizio;

- Rivendita da parte di terzi dei dati personali del cliente ad altre società;

- Combinazione dei dati dei clienti da parte di terzi per compiere un furto di identità.

[30]Direttiva (Ue) 2015/2366 del 25 novembre 2015, relativa a "i servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/Ue e il regolamento (Ue) n. 1093/2010, e abroga la direttiva 2007/64/CE".

Sono alcuni rischi che gravano sulla Banca, e non sul terzo, perché titolare del trattamento e in quanto tale deve proteggere i dati personali che i clienti hanno consentito di trattare. A tal fine è di fondamentale aiuto al titolare del trattamento lo svolgimento della Valutazione di impatto sulla protezione dei dati che deve avvenire in via preliminare al trattamento stesso.
In merito è stata condotta la valutazione di impatto sulla protezione dei dati applicando il modello CoSo Report, come in tutti i precedenti settori d'altronde, la quale viene inserita nell'allegato presente al capitolo 5.

Una volta poste in essere tutte le attività di controllo concernenti il trattamento e calcolato il rischio residuo, si arriva a determinare lo scoring residuo medio. Tale scoring risulta essere mediamente elevato per il trattamento che la banca intende fare.

Privacy					
DISTRIBUZIONE DEI RISCHI PER INDICE DI RISCHIO POTENZIALE E SCORING RESIDUO					
Scoring residuo	Indice di Rischio Potenziale				Totale Rischi
	Continuità	Alto	Medio	Basso	
5	0	0	0	0	0
4	0	7	0	0	7
2	0	5	2	0	7
1	0	7	2	0	9
0	0	2	0	0	2
Totale Rischi	0	21	4	0	25
SCORING RESIDUO MEDIO					
2,04	Mediamente elevato				

Figura 4.9: *Calcolo dello scoring residuo medio concernente il trattamento dei dati personali nell'ambito bancario.*

4.7 Conclusioni della Valutazione d'impatto sulla protezione dei dati

La DPIA viene effettuata prima di iniziare il trattamento dei dati personali proprio perché è uno strumento utile al titolare finalizzato alla valutazione del rischio inerente al trattamento stesso. Come si evince dall'applicazione del modello di DPIA all'interno di vari settori tra loro diversi, eppure accomunati dallo stesso iter procedurale nella valutazione d'impatto, il risultato finale è lo scoring residuo medio. Lo scoring residuo medio non è

altro che lo scoring complessivo del trattamento dato dalla media dei singoli scoring di ciascun elemento preso in considerazione. Lo scoring a sua volta è la trasformazione del rischio residuo di ciascun elemento presente nella colonna degli adempimenti.
Ritornando al risultato complessivo della valutazione, lo scoring residuo medio, questo può essere espresso attraverso cinque giudizi: basso, mediamente basso, mediamente elevato, elevato, di continuità. Sulla base del giudizio emerso l'organizzazione attua le misure necessarie per la mitigazione del rischio, considerando i costi di attuazione. Se nel caso, le misure di sicurezza adottate e l'utilizzo delle tecnologie a disposizione non fosse sufficienti per abbassare il livello di rischio, allora il titolare del trattamento deve consultare l'Autorità di controllo in via preliminare al trattamento (Consultazione preventiva – articolo 36, GDPR). Al Garante devono essere fornite una serie di informazioni, ossia:

"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 previsto;*

c) *le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;*

d) *ove applicabile, i dati di contatto del responsabile della protezione dei dati;*

e) *la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e*

f) *ogni altra informazione richiesta dall'autorità di controllo.*"

L'Autorità di controllo a sua volta *"fornisce entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione."*

Si tiene a puntualizzare il fatto che il Garante viene consultato una volta conclusa la valutazione d'impatto e il suo intervento sarà ex post, ovvero si collocherà in seguito alle determinazioni assunte dal titolare in maniera autonoma. Il motivo risiede nel principio della responsabilizzazione, come è stato ripetuto più volte nel corso della presente dissertazione, principio cardine alla base del Regolamento UE, che lascia piena libertà al titolare nella gestione dei dati personali. Infatti, è il titolare che chiede la consultazione

al Garante una volta cosciente dei rischi inerenti al trattamento per i diritti e le libertà degli interessati. L'autorità di controllo, nel rispetto del principio dell'*accountability*, lascia piena autonomia al titolare, ed interviene solo su richiesta di quest'ultimo. Quando viene consultato il Garante in merito alla DPIA può decidere se applicare i poteri conferiti ai sensi dell'articolo 58 o autorizzare il titolare ad effettuare il trattamento valutato.

Per quanto riguarda la pubblicazione della Valutazione d'impatto sulla protezione dei dati, essa non è obbligatoria, tuttavia costituisce una punto a favore dell'organizzazione che la pubblica in termini di fiducia verso i clienti e anche verso i terzi.

In merito all'inosservanza a quanto previsto agli artt. 35 e 36, ovvero omettere la DPIA quando invece si è obbligati a svolgerla e non consultare il Garante quando invece si deve consultare, questa è punita con una sanzione amministrativa pecuniaria fino a 10 milioni di euro, o nel caso delle imprese fino al 2 percento del fatturato annuo (articolo 83, paragrafo 4, lett. a)).

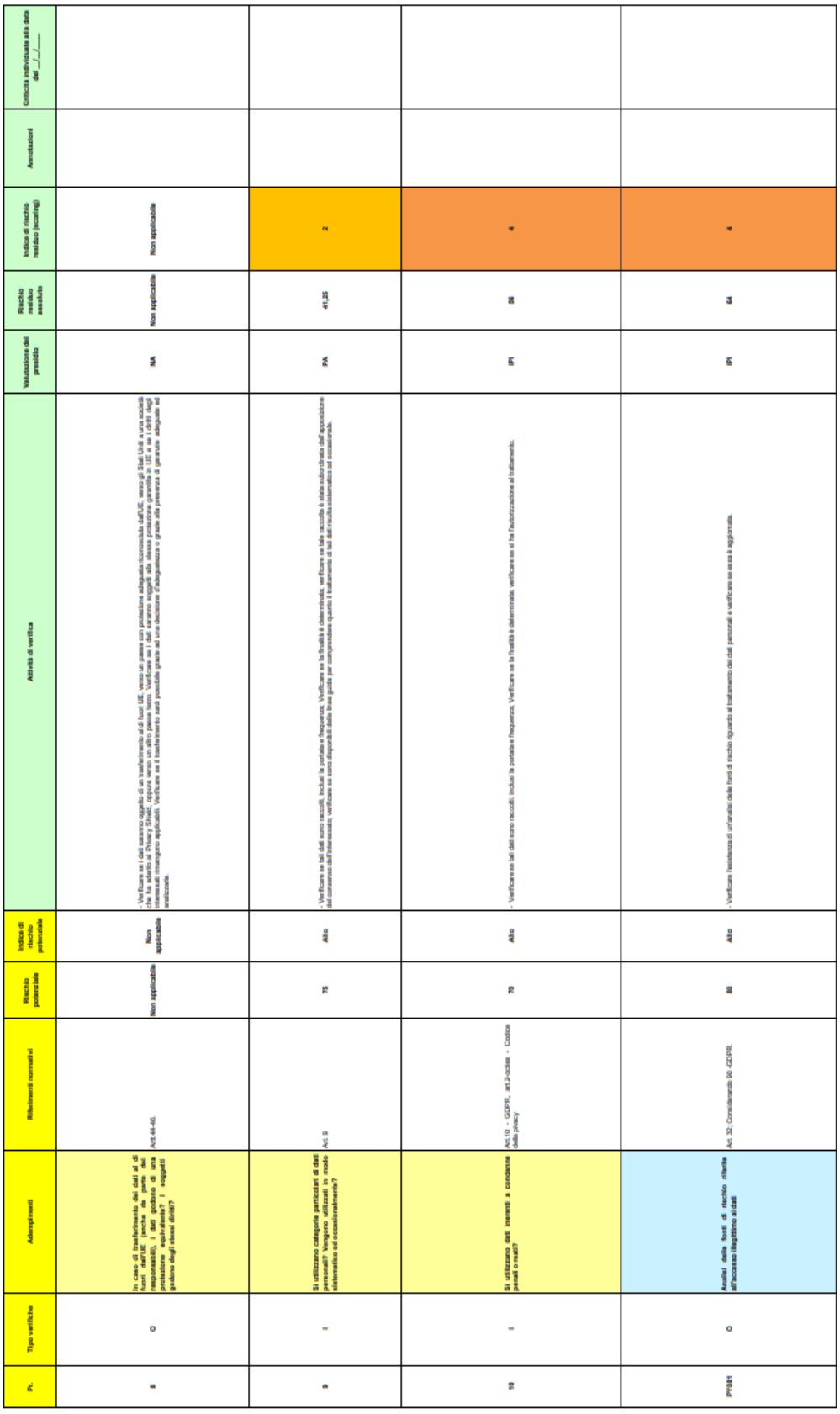
Capitolo 5

Le Tabelle relative al Modello di DPIA

Il presente capitolo contiene tutte le tabelle relative al modello di Valutazione d'impatto sulla protezione dei dati applicato ai quattro scenari diversi analizzati nel precedente capitolo.

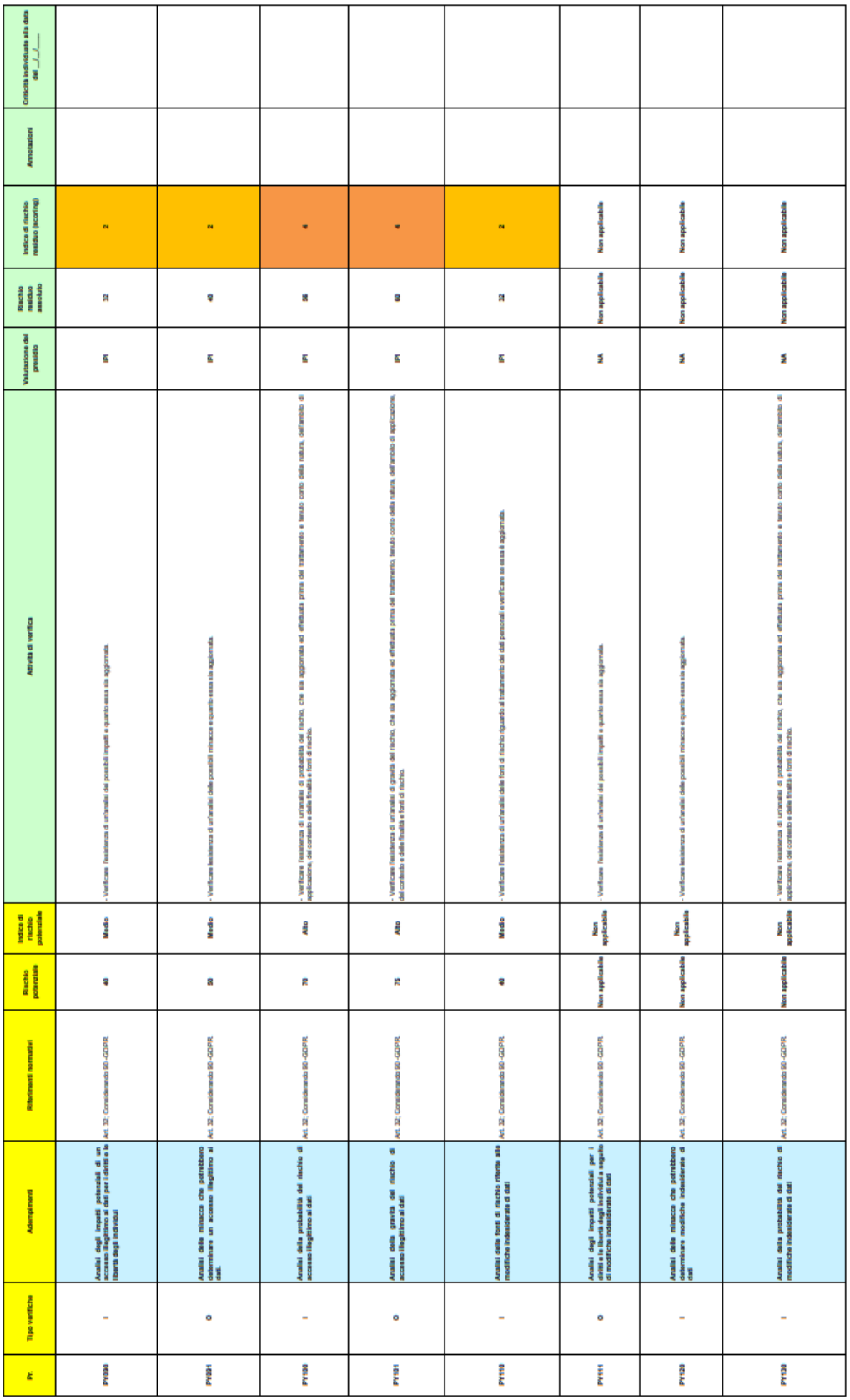
Pr.	Tipo verifiche	Adempimenti	Riferimenti normativi	Rischio potenziale	Indice di rischio potenziale	Attività di verifica	Valutazione del presidio	Rischio residuo assoluto	Indice di rischio residuo (scoring)	Annotazioni	Criticità individuate alla data del __/__/____
1	I	La base legale per il trattamento è determinata correttamente?	art.6, paragrafo 1, - GDPR	80	Alto	- Verificare se l'interessato ha acconsentito al trattamento dei dati personali per lo scopo specifico considerato; - Verificare se il trattamento è necessario per l'esecuzione delle misure preliminari per la stipula di un contratto o per l'esecuzione di un contratto di cui l'interessato è parte; - verificare se il trattamento è necessario ai fini della legge.	PA	44	2	Parte che viene compilata durante il trattamento, in quanto la DPIA è un processo dinamico che deve essere monitorato e aggiornato.	Come le annotazioni. Si segnano tutti gli intoppi riscontrati durante il trattamento.
2	I	I dati vengono usati solo per scopi specifici?	art.5, paragrafo 1, lett. b) - GDPR	70	Alto	- Verificare che i dati siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.	A	7	0		
3	I	I dati raccolti sono limitati e non eccessivi?	art.5, paragrafo 1, lett. c) - "Minimizzazione dei dati"	75	Alto	- Verificare che non vi siano dati o consensi raccolti in più rispetto alla finalità del trattamento.	A	7,5	0		
4	I	i dati raccolti sono esatti e aggiornati?	art. 5, paragrafo 1, lett. d)	70	Alto	- Verificare la correttezza e l'aggiornamento dei dati personali trattati. - Verificare la corretta conservazione delle copie dei documenti utilizzati per l'identificazione.	PA	38,5	2		
5	O	Il periodo di conservazione dei dati è in linea con le finalità e con la legge?	art. 5, paragrafo 1, lett. e)	80	Alto	Verificare se il periodo di conservazione dei dati è calcolato in modo corretto e verificare a campione se il periodo di conservazione è rispettato	PA	44	2		
6	I	Gli interessati han dato il consenso al trattamento (ove necessario)? sono stati informati in modo appropriato sulle finalità, sui propri diritti e su come esercitarli?	artt. 7, 12, 13, 14, 15-22.	70	Alto	"- Verificare l'esistenza di una funzione aziendale responsabile della predisposizione dell'informativa sulla privacy e del suo aggiornamento. - Verificare l'esistenza/adeguatezza di una procedura interna che definisca le modalità di predisposizione e stampa delle informative sulla privacy e di raccolta del consenso al trattamento dei dati. In particolare verificare che la suddetta procedura disciplini che il consenso sia informato, libero (non "pre-opzionato"), specifico, espresso e documentato in forma scritta. - Verificare l'esistenza/adeguatezza di una procedura interna che definisca le modalità con cui rendere noti eventuali aggiornamenti dell'informativa con comunicazioni periodiche nonché sull'eventuale sito internet della banca. - Verificare l'esistenza/adeguatezza di un supporto informatico che consenta, al momento della instaurazione del rapporto col cliente, la stampa della relativa informativa sulla privacy. Verificare, inoltre, che l'informativa stampabile sia coerente con le previsioni contrattuali (quindi che non si raccolgano più consensi di quelli necessari) definite e sia aggiornata rispetto agli obblighi imposti dalla normativa sulla privacy. - Verificare l'esistenza/adeguatezza di una procedura interna che subordini il trattamento relativo alle attività bancarie richieste dal cliente al relativo e preventivo consenso del cliente stesso. - Verificare che la banca abbia previamente informato l'interessato o la persona presso la quale sono stati raccolti i dati personali circa: - le finalità e modalità del trattamento; - natura obbligatoria o facoltativa del conferimento dei dati; - le conseguenze di un eventuale rifiuto; - i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi (compreso l'estero); - i diritti di cui gli artt. 15-22 e come esercitarli; -diritto di reclamo all'Autorità; - gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato e del responsabile; - l'esistenza di un processo decisionale automatizzato. Se non vi è il consenso, verificare se la motivazione dello SFORZO	IPA	21	1		
7	O	Gli obblighi dei responsabili del trattamento sono stati definiti da contratto? Vi è stata una effettiva designazione per iscritto di tutti gli incaricati del trattamento (dipendenti, collaboratori, lavoratori interinali, consulenti, ecc.) e individuazione puntuale dell'ambito di trattamento.	Artt. 28, 29.	80	Alto	- Verificare l'esistenza/adeguatezza di una procedura interna che regolamenti la nomina dell'i responsabile/i del trattamento. - Verificare che la procedura di designazione preveda la nomina con atto scritto del Responsabile e impartisca le relative istruzioni ai sensi dell'articolo 28. - Verificare che sia stata svolta una valutazione sull'esperienza, capacità e affidabilità del responsabile designato. "- Verificare l'esistenza di una procedura aziendale preposta alla designazione, e aggiornamento, degli incaricati al trattamento dei dati e dei relativi poteri e responsabilità loro riconosciuti. - Verificare l'esistenza/adeguatezza di una procedura interna che individui i soggetti che per mansioni e responsabilità svolte devono essere incaricati del trattamento dati. Inoltre verificare che siano formalizzati i compiti e le responsabilità degli incaricati designati. A tal proposito verificare che la suddetta procedura di designazione preveda la nomina con atto scritto dell'incaricato e individui puntualmente l'ambito del trattamento consentito. - Verificare l'esistenza/adeguatezza di una procedura interna che consenta il controllo della coerenza tra profilazione utente e mansioni attribuite.	PA	44	2		

Figura 5.1: Check-list relativa alla Videosorveglianza - parte 1



Pr.	Tips verifiche	Adempimenti	Riferimenti normativi	Rischio potenziale	Indice di rischio potenziale	Attività di verifica	Valutazione del presidio	Rischio residuo assoluto	Indice di rischio residuo (scoring)	Annotazioni	Criticità individuate alla data del __/__/____
8	O	In caso di trasferimento dei dati al di fuori dell'UE (anche da parte dei responsabili), i dati godono di una protezione analoga? I soggetti godono degli stessi diritti?	Art.44-46	Non applicabile	Non applicabile	- Verificare sui dati soggetti di un trasferimento ed il loro UE, verso un paese con protezione adeguata riconosciuta dall'UE, verso gli Stati Uniti a cura poiché che ha aderito al Privacy Shield, oppure verso un altro paese terzo. Verificare se i dati saranno soggetti alla stessa protezione, garantita in UE, e se i diritti degli interessati rimangono applicabili. Verificare se il trasferimento sarà possibile grazie ad una decisione d'adeguatezza o grazie alla presenza di garanzie adeguate ed applicabili.	NA	Non applicabile	Non applicabile		
9	I	Si utilizzano categorie particolari di dati personali? Vengono utilizzati in modo sistematico od occasionalmente?	Art. 9	75	Alto	- Verificare sui tali dati sono raccolti, inclusi la portata e frequenza; Verificare sia la finalità è determinata; verificare se tale raccolta è stata subordinata dall'apposizione del consenso dell'interessato; verificare se sono disponibili dalle linee guida per comprendere quando il trattamento di tali dati risulta sistematico od occasionale.	PA	41,25	2		
10	I	Si utilizzano dati biometrici a condanne penali o reati?	Art.10 - GDPR, art.2-octies - Codice della privacy	79	Alto	- Verificare sui tali dati sono raccolti, inclusi la portata e frequenza; Verificare sia la finalità è determinata; verificare se si ha l'autorizzazione al trattamento.	PI	56	4		
PYS01	O	Analisi delle fonti di rischio riferite all'accesso illegittimo ai dati	Art. 32; Considerando 90 -GDPR	88	Alto	- Verificare l'esistenza di un'analisi delle fonti di rischio riguardo al trattamento dei dati personali e verificare se essa è aggiornata.	PI	64	4		

Figura 5.2: Check-list relativa alla Videosorveglianza - parte 2



Pr.	Tipo verifiche	Adempimenti	Riferimenti normativi	Rischio potenziale	Indice di rischio potenziale	Attività di verifica	Valutazione del presidio	Rischio residuo assunto	Indice di rischio residuo (scoring)	Annotazioni	Criticità individuate alla data del __/__/____
PY090	I	Analisi degli impatti potenziali di un accesso illegittimo ai dati per i diritti e le libertà degli individui	Art. 32; Considerando 83 GDPR	49	Medio	- Verificare l'esistenza di un'analisi dei possibili impatti e quanto essa sia aggiornata.	PI	32	2		
PY091	O	Analisi della minaccia che potrebbero determinare un accesso illegittimo ai dati.	Art. 32; Considerando 83 GDPR	69	Medio	- Verificare l'esistenza di un'analisi delle possibili minacce e quanto essa sia aggiornata.	PI	49	2		
PY100	I	Analisi della probabilità del rischio di accesso illegittimo ai dati	Art. 32; Considerando 83 GDPR	79	Alto	- Verificare l'esistenza di un'analisi di probabilità del rischio, che sia aggiornata ed effettuata prima del trattamento e tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità e fonti di rischio.	PI	56	4		
PY101	O	Analisi della gravità del rischio di accesso illegittimo ai dati	Art. 32; Considerando 83 GDPR	75	Alto	- Verificare l'esistenza di un'analisi di gravità del rischio, che sia aggiornata ed effettuata prima del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità e fonti di rischio.	PI	69	4		
PY110	I	Analisi delle fonti di rischio relative alle modifiche indesiderate di dati	Art. 32; Considerando 83 GDPR	49	Medio	- Verificare l'esistenza di un'analisi delle fonti di rischio riguardo al trattamento dei dati personali e verificare se essa è aggiornata.	PI	32	2		
PY111	O	Analisi degli impatti potenziali per i diritti e le libertà degli individui a seguito di modifiche indesiderate di dati	Art. 32; Considerando 83 GDPR	Non applicabile	Non applicabile	- Verificare l'esistenza di un'analisi dei possibili impatti e quanto essa sia aggiornata.	NA	Non applicabile	Non applicabile		
PY120	I	Analisi della minaccia che potrebbero determinare modifiche indesiderate di dati	Art. 32; Considerando 83 GDPR	Non applicabile	Non applicabile	- Verificare l'esistenza di un'analisi delle possibili minacce e quanto essa sia aggiornata.	NA	Non applicabile	Non applicabile		
PY130	I	Analisi della probabilità del rischio di modifiche indesiderate di dati	Art. 32; Considerando 83 GDPR	Non applicabile	Non applicabile	- Verificare l'esistenza di un'analisi di probabilità del rischio, che sia aggiornata ed effettuata prima del trattamento e tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità e fonti di rischio.	NA	Non applicabile	Non applicabile		

Figura 5.3: Check-list relativa alla Videosorveglianza - parte 3

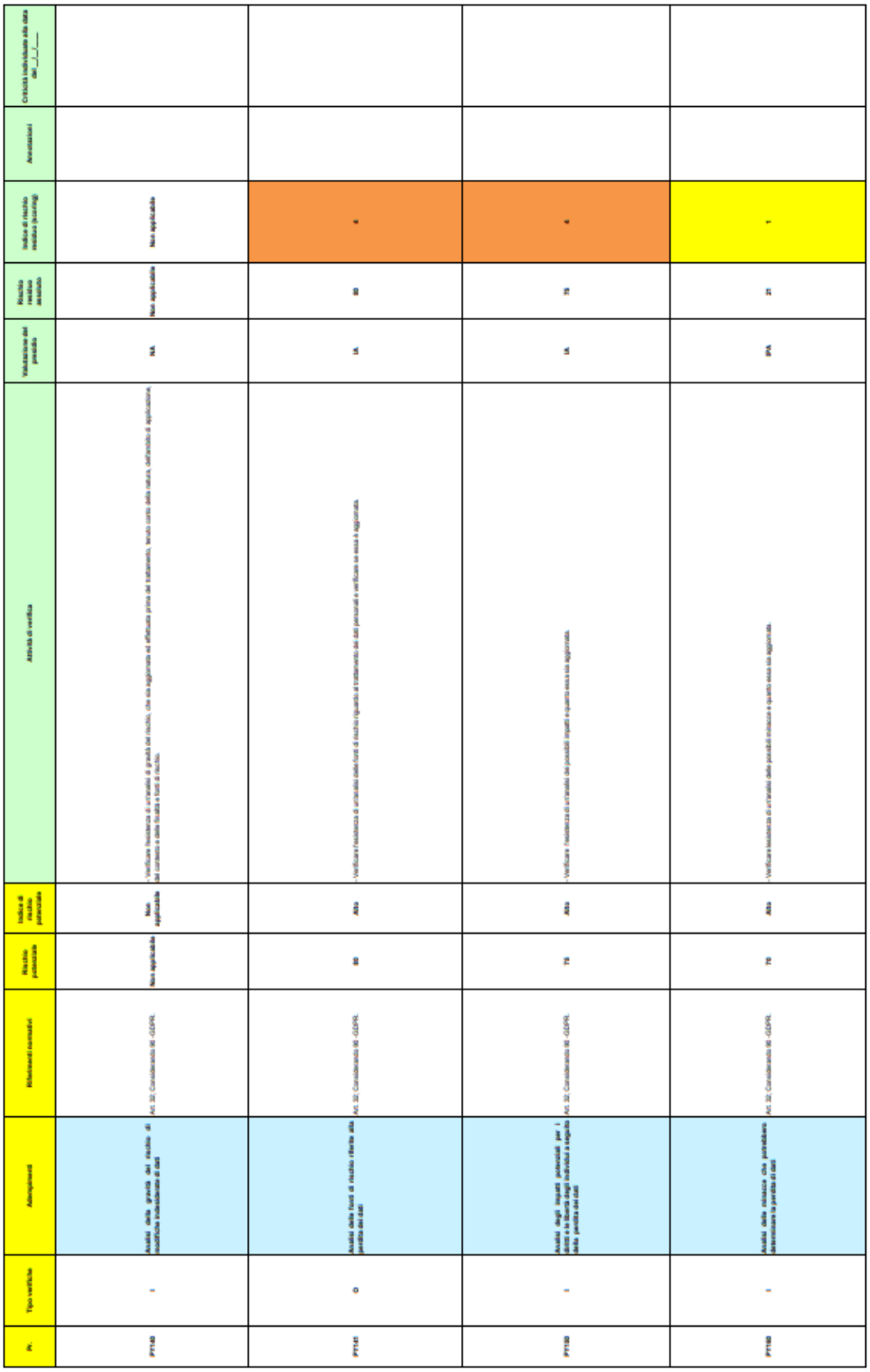
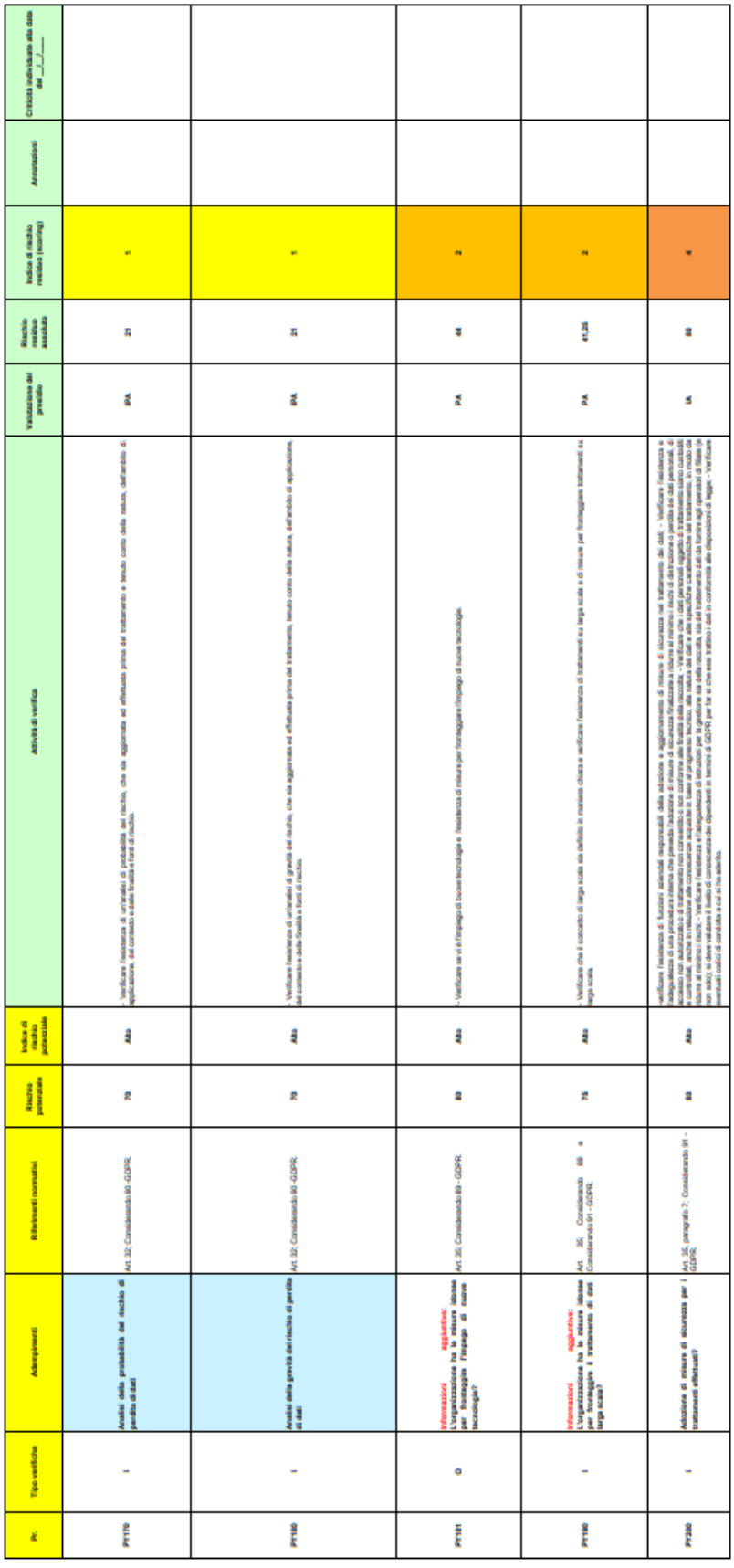


Figura 5.4: Check-list relativa alla Videosorveglianza - parte 4



Pr.	Tipo verifica	Adempimenti	Riferimenti normativi	Rischio potenziale	Indice di rischio potenziale	Attività di verifica	Valutazione del pregiudizio	Rischio residuo assoluto	Indice di rischio residuo (ricalcolato)	Annotazioni	Criticità individuate alla data dd / /
P170	I	Analisi della probabilità del rischio di perdita di dati	Art. 32; Considerando 83 -GDPR;	79	Alto	- Verificare l'esistenza di un'analisi di probabilità del rischio, che sia aggiornata ed effettuata prima del trattamento e tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità e fonti di rischio.	IPA	21	1		
P150	I	Analisi della gravità del rischio di perdita di dati	Art. 32; Considerando 83 -GDPR;	79	Alto	- Verificare l'esistenza di un'analisi di gravità del rischio, che sia aggiornata ed effettuata prima del trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità e fonti di rischio.	IPA	21	1		
P161	O	**Informazioni aggiuntive:** L'organizzazione ha le misure idonee per fronteggiare l'impiego di nuove tecnologie?	Art 35; Considerando 89 -GDPR;	88	Alto	- Verificare se vi è l'impiego di nuove tecnologie e - l'esistenza di misure per fronteggiare l'impiego di nuove tecnologie.	PA	44	2		
P190	I	**Informazioni aggiuntive:** L'organizzazione ha le misure idonee per fronteggiare il trattamento di dati larga scala?	Art. 35; Considerando 89 e Considerando 91 -GDPR;	75	Alto	- Verificare che il concetto di larga scala sia definito in maniera chiara e verificare l'esistenza di trattamenti su larga scala e di misure per fronteggiare trattamenti su larga scala.	PA	41,25	2		
P230	I	Adozione di misure di sicurezza per i trattamenti effettuati?	Art 36, paragrafo 7; Considerando 91 - GDPR;	88	Alto	verificare l'esistenza di funzioni aziendali responsabili della adozione e aggiornamento di misure di sicurezza nel trattamento dei dati; - Verificare l'esistenza e l'adeguatezza di una procedura interna che preveda l'adozione di misure di sicurezza finalizzate a ridurre al minimo i rischi di distruzione o perdita dei dati personali, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta; - Verificare che i dati personali oggetto di trattamento siano custoditi e controllati mediante misure di sicurezza tali da ridurre al minimo i rischi di distruzione o perdita, anche accidentale, dei dati stessi, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta; - Verificare che siano adottate misure di sicurezza idonee a ridurre al minimo i rischi; - Verificare l'esistenza e l'adeguatezza di istruzioni per la gestione sia della raccolta, sia del trattamento dati da fornire agli operatori di filiale (e non solo), e deve valutare il livello di conoscenza dei dipendenti in tema di GDPR per far sì che essi trattino i dati in conformità alle disposizioni di legge; - Verificare eventuali codici di condotta a cui si ha aderito.	IA	88	4		

Figura 5.5: Check-list relativa alla Videosorveglianza - parte 5

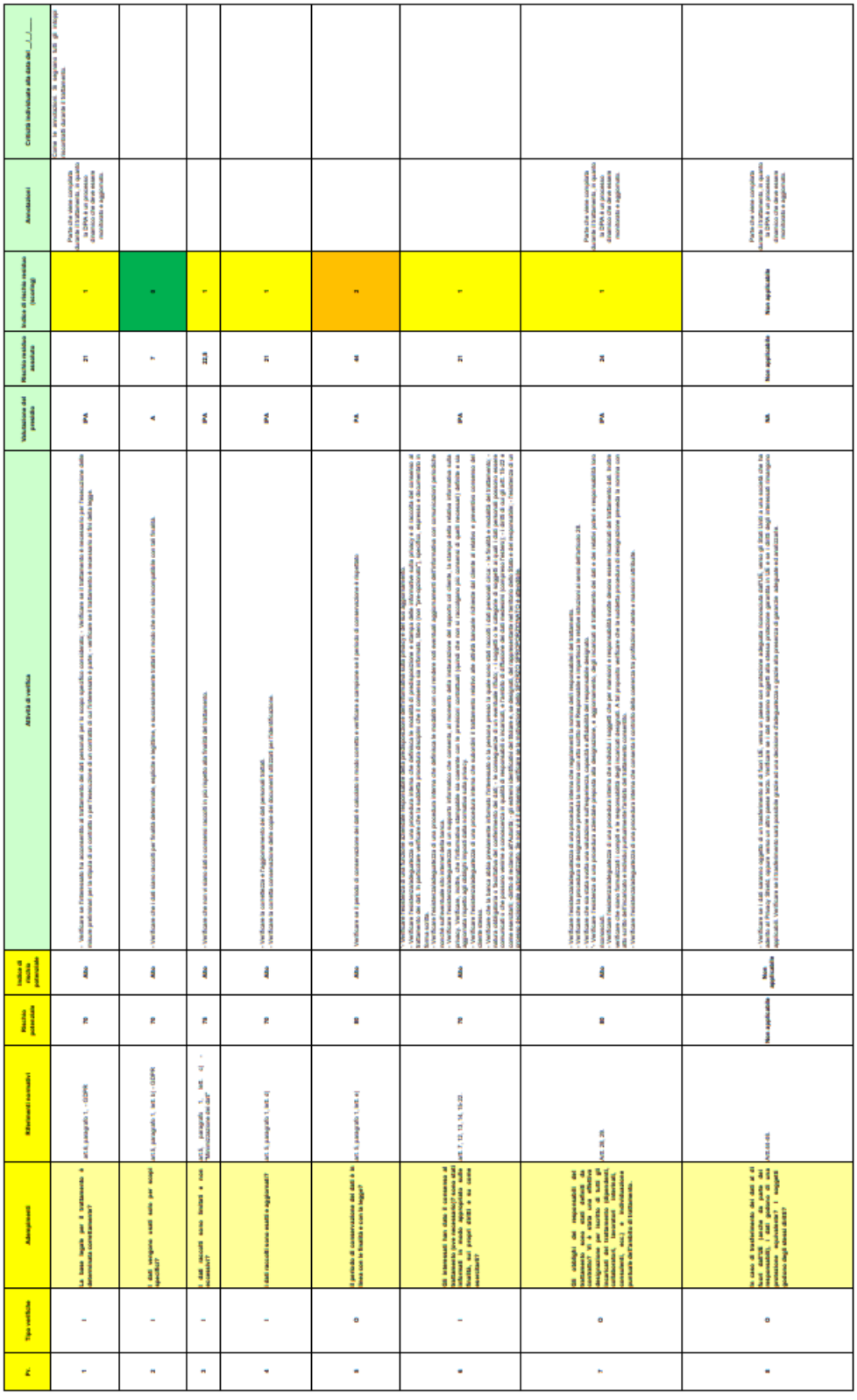


Figura 5.6: Check-list relativa al trattamento dei dati nell'azienda ospedaliera - parte 1

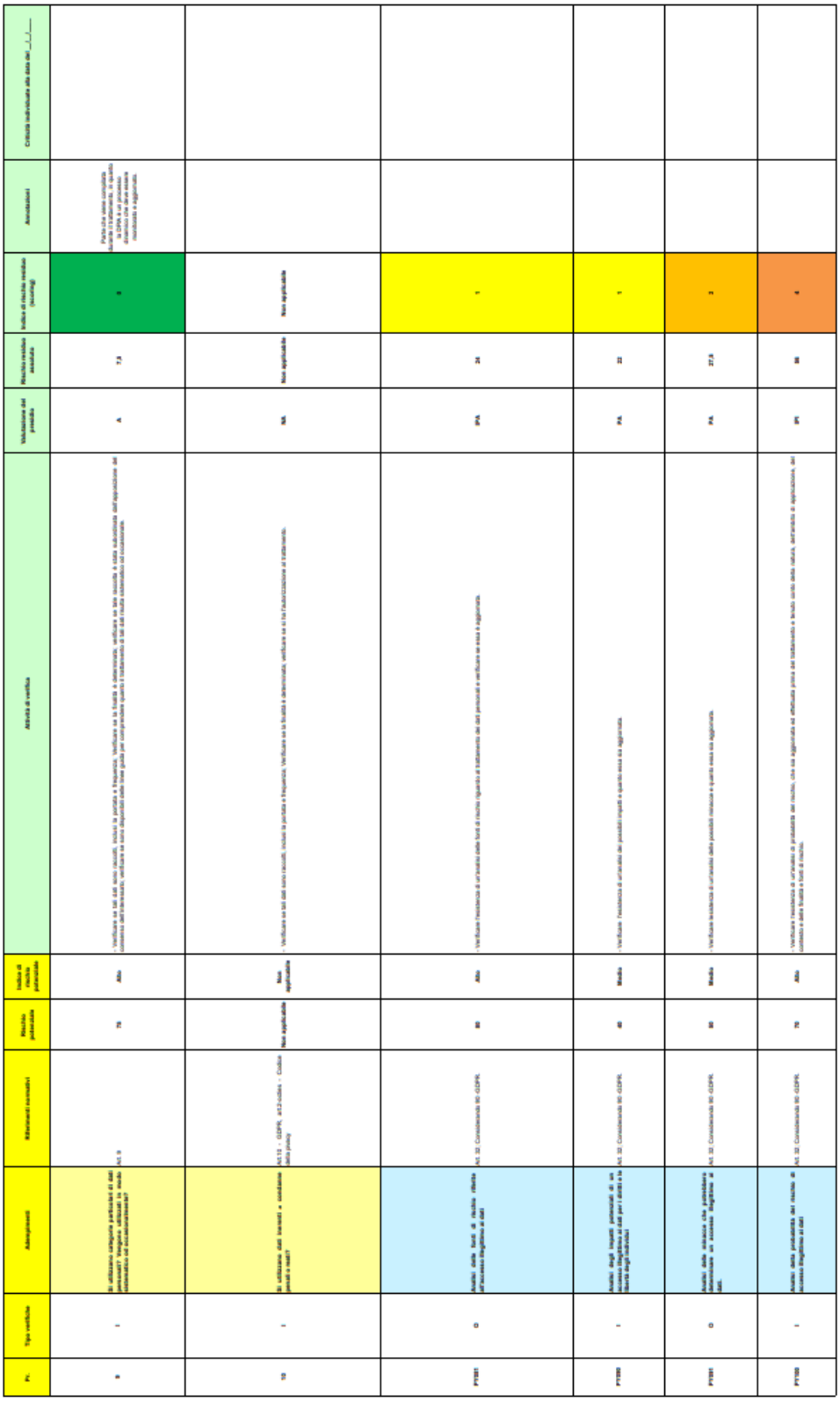


Figura 5.7: Check-list relativa al trattamento dei dati nell'azienda ospedaliera - parte 2

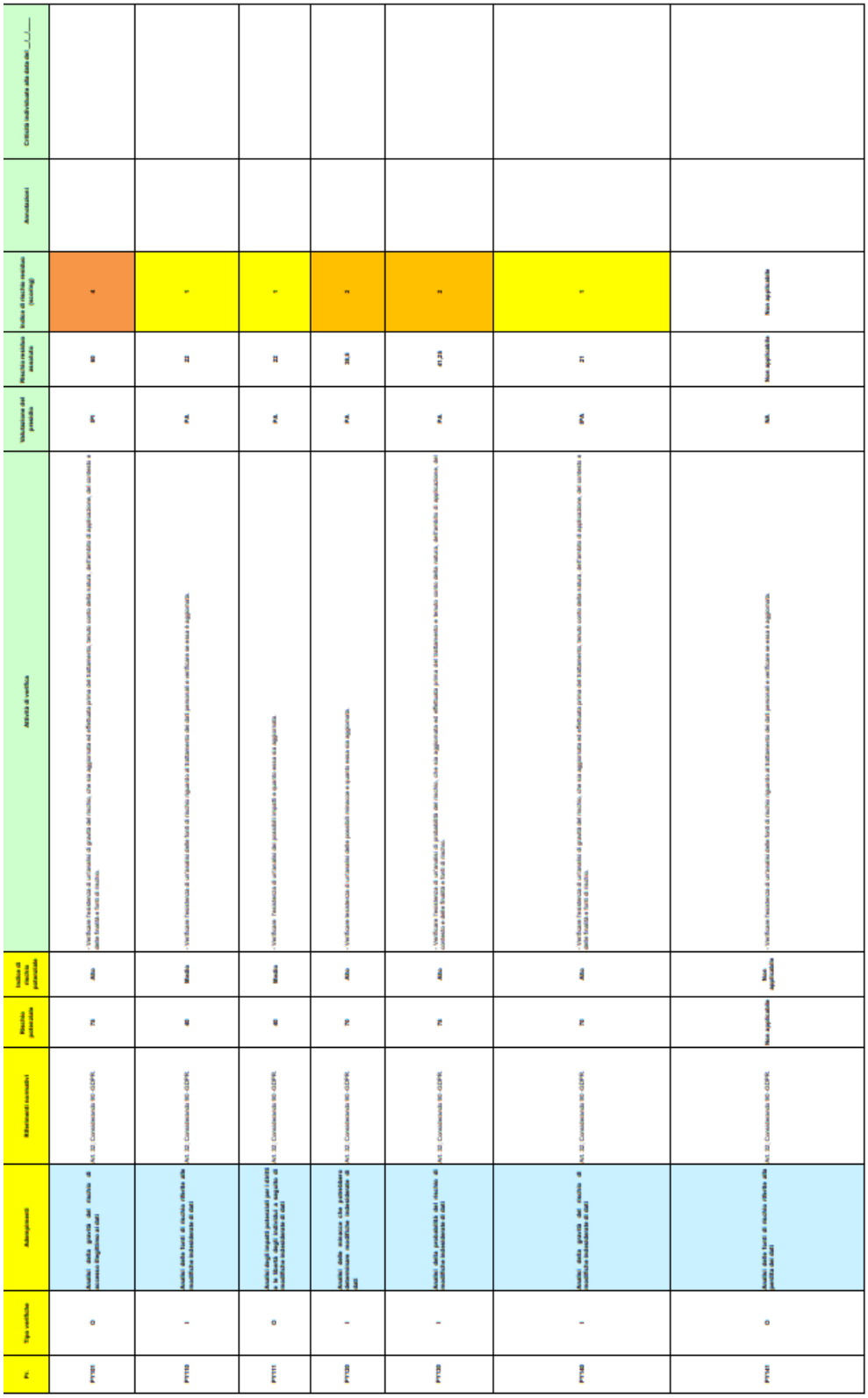


Figura 5.8: Check-list relativa al trattamento dei dati nell'azienda ospedaliera - parte 3

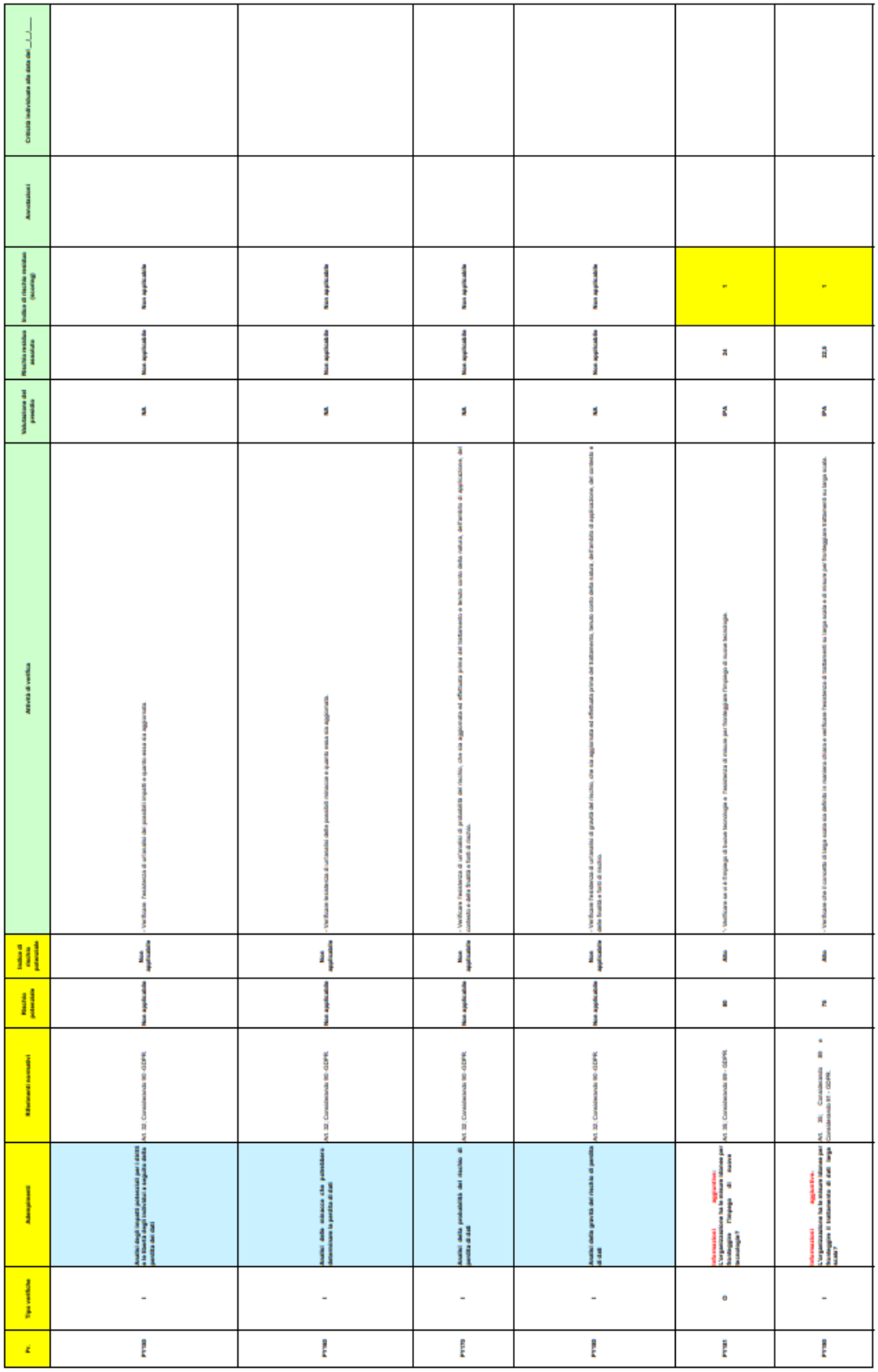


Figura 5.9: Check-list relativa al trattamento dei dati nell'azienda ospedaliera - parte 4

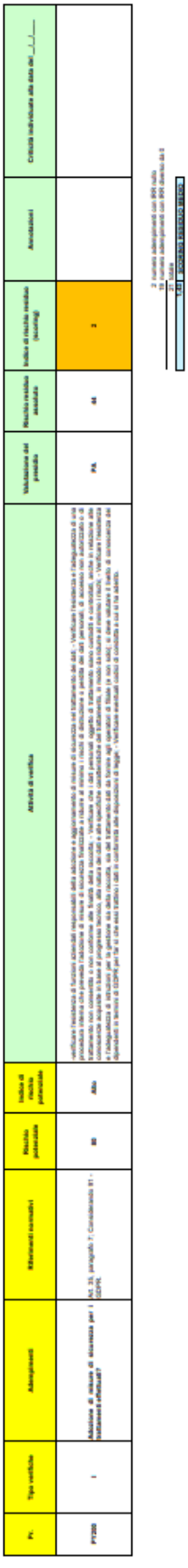


Figura 5.10: Check-list relativa al trattamento dei dati nell'azienda ospedaliera - parte 5

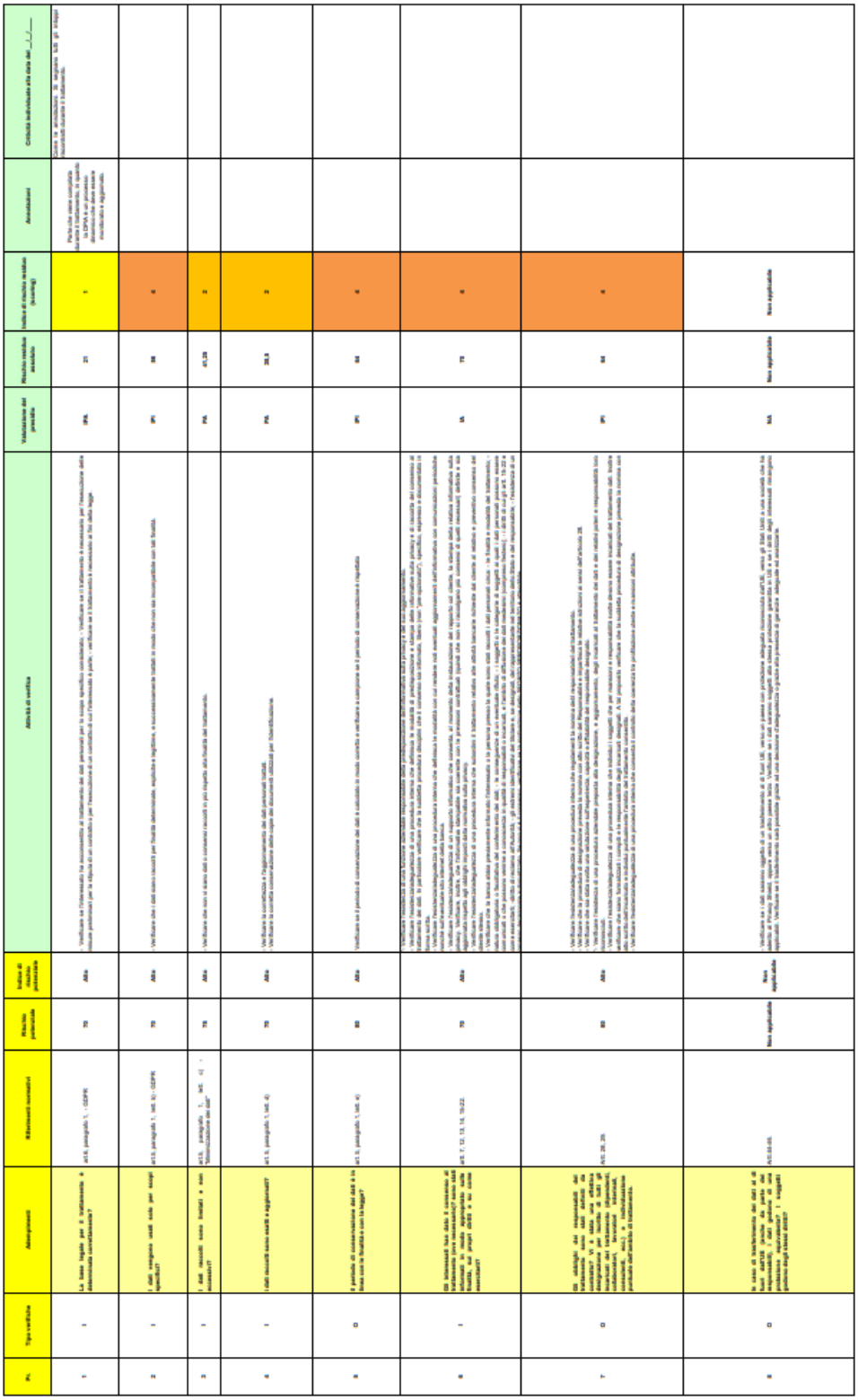


Figura 5.11: Check-list relativa al trattamento dei dati nel settore del Telemarketing - parte 1

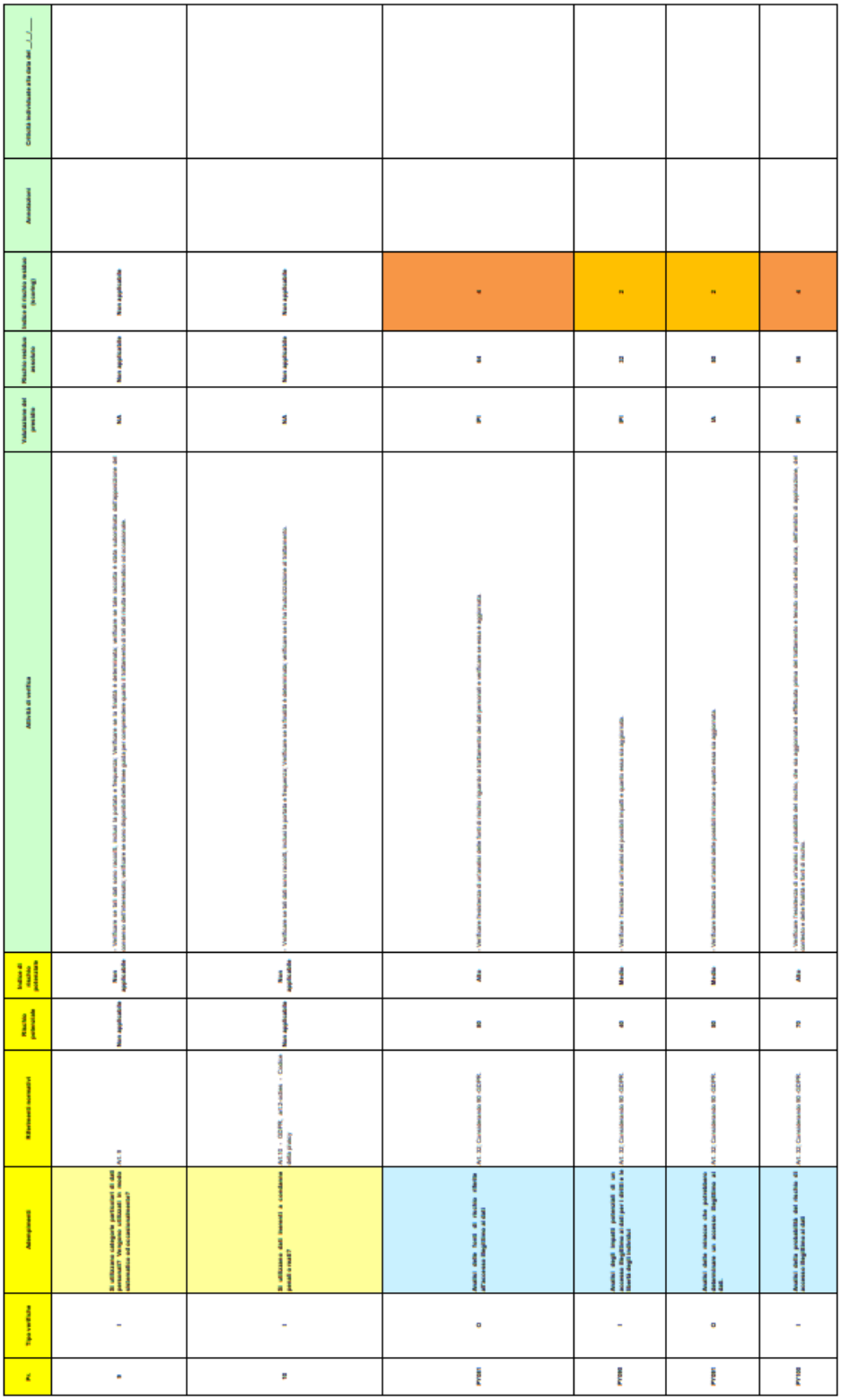


Figura 5.12: Check-list relativa al trattamento dei dati nel settore del Telemarketing - parte 2

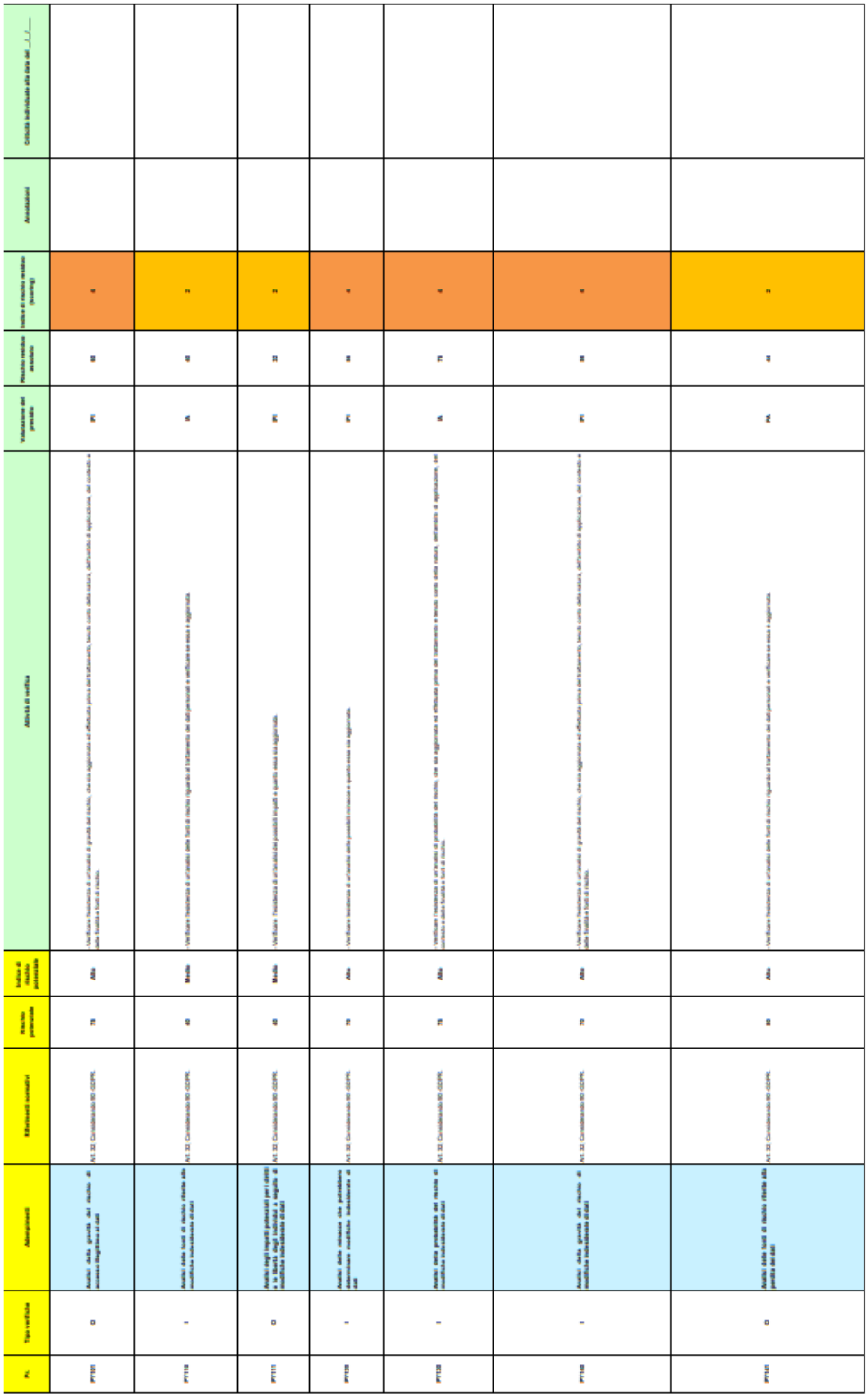


Figura 5.13: Check-list relativa al trattamento dei dati nel settore del Telemarketing - parte 3

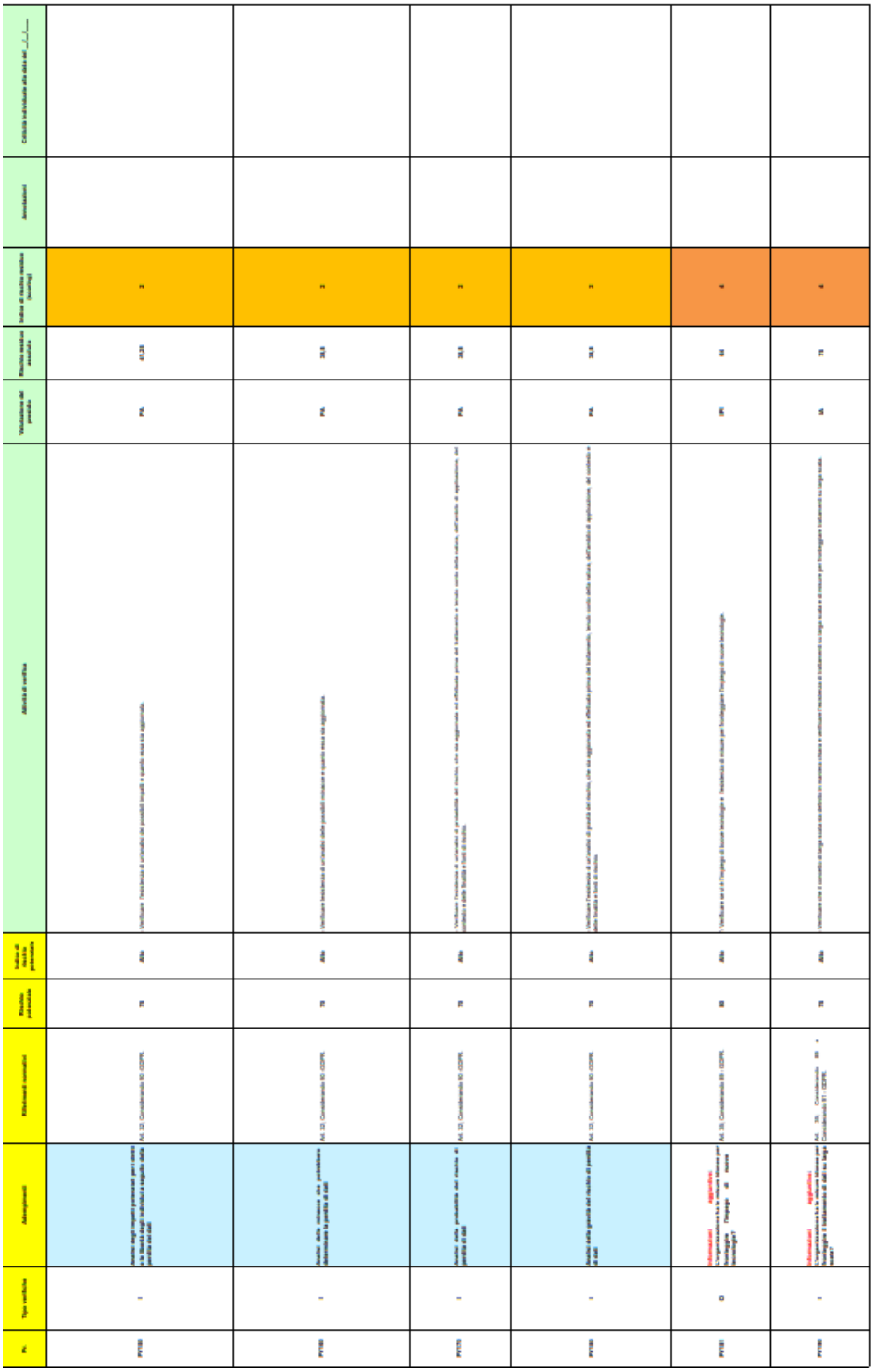


Figura 5.14: Check-list relativa al trattamento dei dati nel settore del Telemarketing - parte 4

Figura 5.15: Check-list relativa al trattamento dei dati nel settore del Telemarketing - parte 5

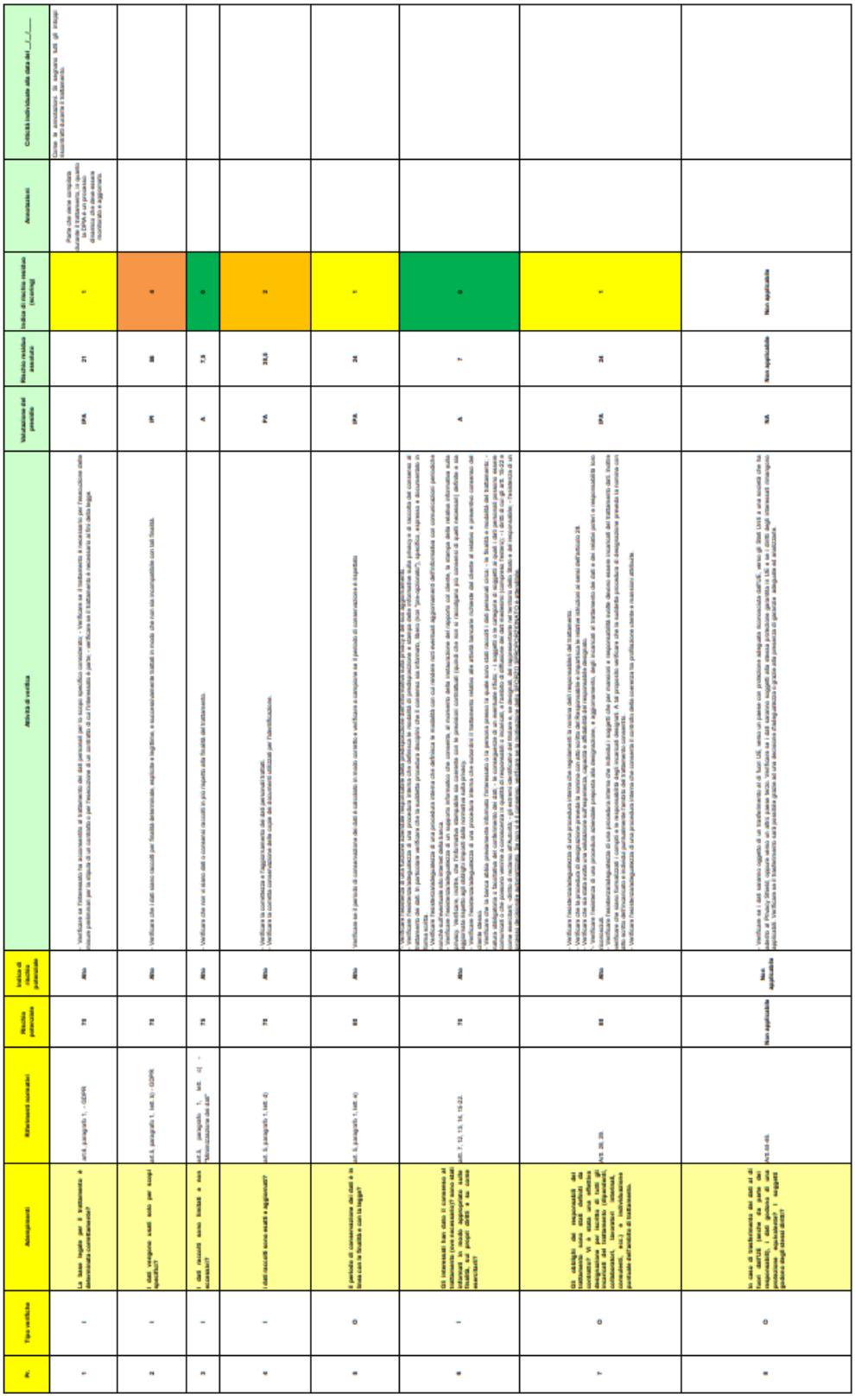


Figura 5.16: Check-list relativa al trattamento dei dati nel settore bancario - parte 1

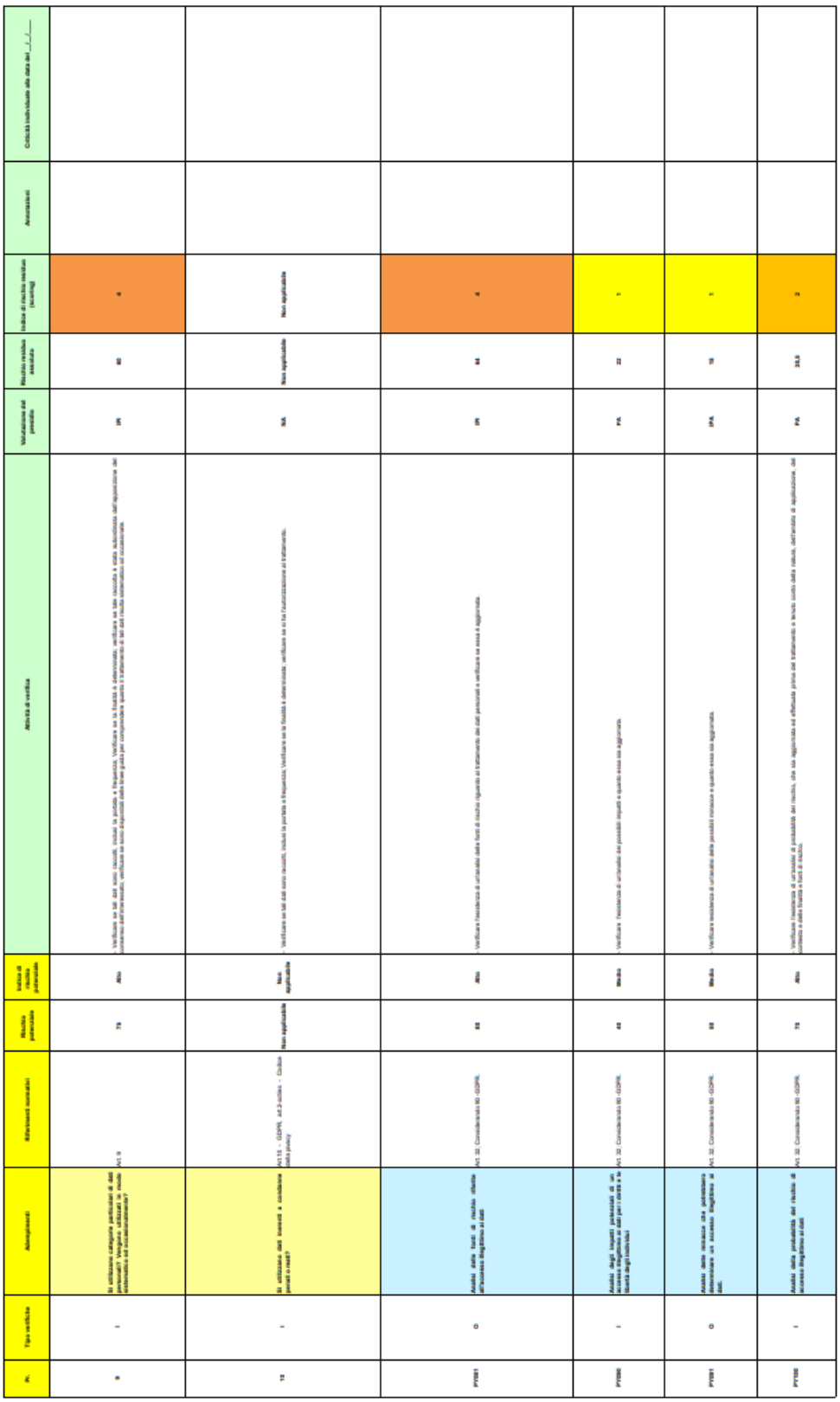


Figura 5.17: Check-list relativa al trattamento dei dati nel settore bancario - parte 2

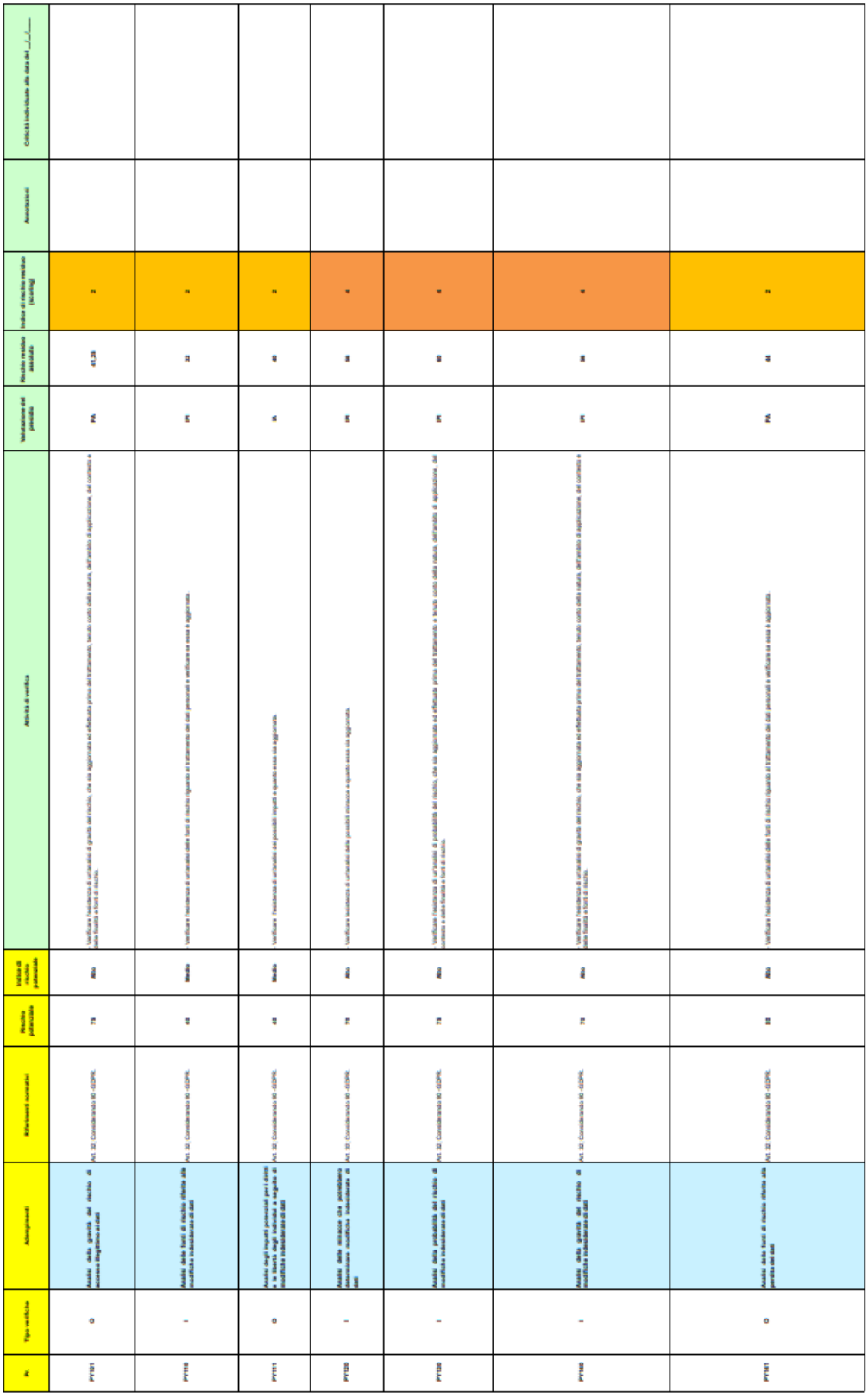


Figura 5.18: Check-list relativa al trattamento dei dati nel settore bancario - parte 3

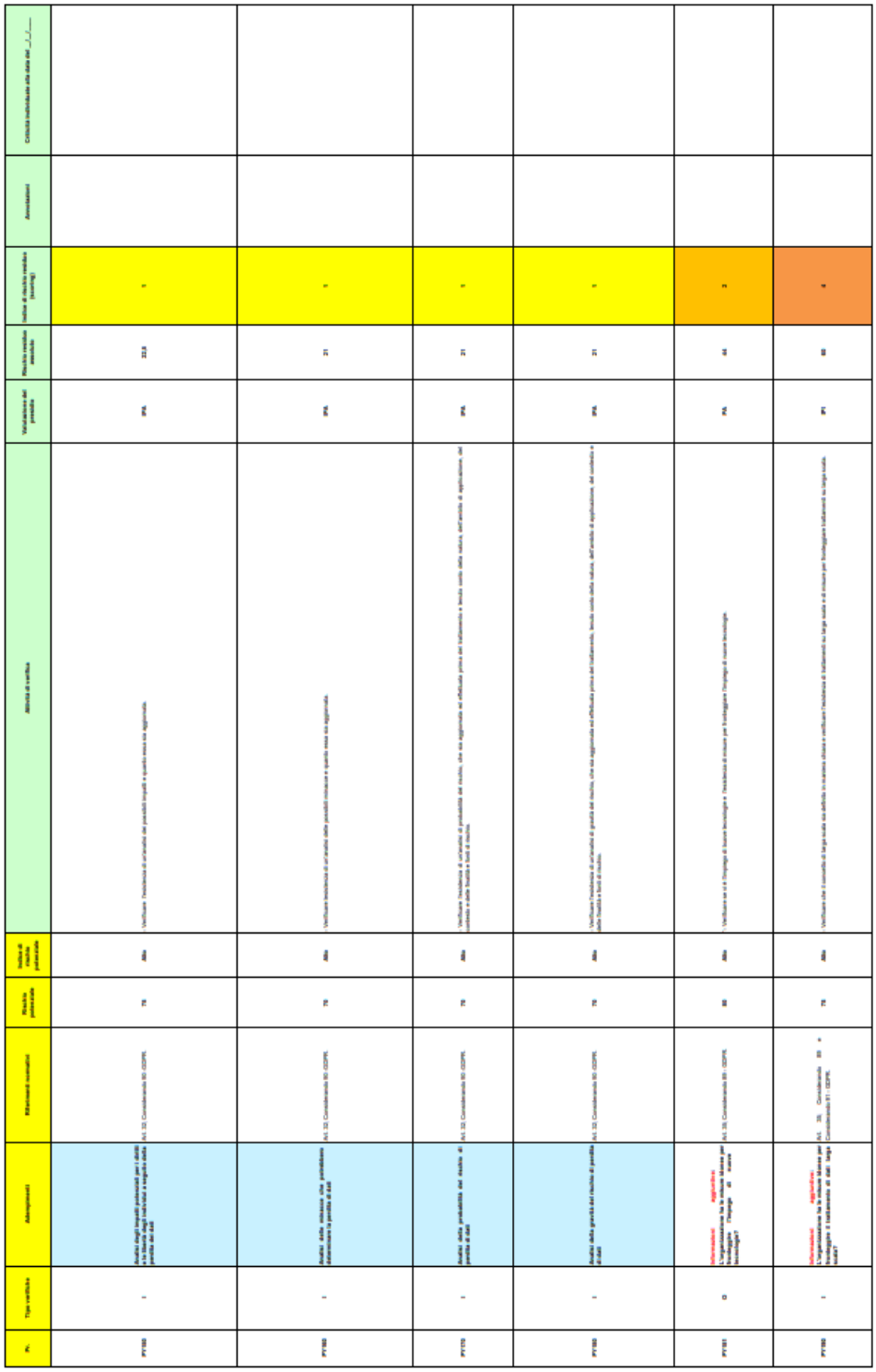


Figura 5.19: Check-list relativa al trattamento dei dati nel settore bancario - parte 4

Figura 5.20: Check-list relativa al trattamento dei dati nel settore bancario - parte 5

Conclusioni

Il presente elaborato è iniziato con l'illustrazione del percorso storico-giuridico del concetto di privacy, il quale si è evoluto fino a diventare diritto fondamentale dell'individuo. In merito a questa evoluzione si è voluto analizzare lo sfondo storico – prima quello statunitense, in seguito quello europeo – per poter apprendere al meglio i motivi dell'adozione del Regolamento UE n.2016/679 in materia di protezione dei dati personali, Regolamento che abroga la Direttiva 95/46/CE in vigore per oltre un ventennio.

La motivazione principale risiede nel progresso tecnologico, il quale capovolge la nozione di privacy intesa come il diritto di essere lasciati da soli – *The right to be let alone* di Brandeis e Warren – fondato sul criterio dell'esclusione degli altri dalla propria sfera privata, nel diritto di controllare come gli altri trattino i propri dati. Il concetto stesso di "sfera privata" si è trasformata per effetto della rivoluzione elettronica *"in un luogo di scambi, di condivisione di dati personali, di informazioni la cui circolazione non riguarda più soltanto quelle in uscita di cui altri possono appropriarsi o venire a conoscenza, ma interessa anche quelli in entrata, con le quali altri invadano quella sfera in forme sempre più massicce e indesiderate e così la modificano continuamente."*[1] Quindi il mondo virtuale ha assunto il ruolo di un vero e proprio ambiente dove si esplicita la propria personalità. In questo scenario si colloca la nuova disciplina europea, che cerca di combinare il progresso tecnologico e la globalizzazione con il diritto alla privacy, imponendo ai Titolari del trattamento livelli di sicurezza adeguati alle diverse tipologie di trattamento di dati personali.

Come si evince, l'intera dissertazione ruota intorno al Regolamento generale sulla protezione dei dati, illustrandone le novità da esso introdotte, come il principio dell'*accountability* – elemento basilare del Regolamento europeo – che investe il Titolare e il Responsabile del trattamento rendendoli più liberi nelle loro scelte di gestione del trattamento, inclusi i rischi inerenti ad esso per i diritti e le libertà dei soggetti interessati. Ma più libertà significa anche più responsabilità in capo al Titolare e al Responsabile del trattamento in quanto devono dimostrare di essere in grado di valutare i rischi connessi all'utilizzo dei dati personali, nonché provvedere alla loro mitigazione grazie all'attuazione di misure di sicurezza

[1] S. RODOTA', *Il mondo nella rete. Quali i diritti, quali i vincoli*, Roma, Laterza, 2014.

idonee.

Tuttavia il legislatore europeo mette a disposizione del titolare una serie di strumenti, i *c.d. "accountability tools"* al fine di sostenere il Titolare nell'attuazione del principio della responsabilizzazione, uno tra questi è la Valutazione d'impatto sulla protezione dei dati, tema centrale del presente elaborato.

La finalità di questa tesi è stata quella di sviluppare un modello di valutazione d'impatto sulla protezione dei dati ai sensi dell'articolo 35 del Regolamento UE n. 2016/679, tenendo in considerazione le Linee guida del Gruppo di Lavoro articolo 29 in merito alla DPIA. Tale modello di DPIA tende a specificare il contenuto dell'articolo 35, paragrafo 7 – GDPR, ossia dare una descrizione sistematica del trattamento considerando la natura, portata, contesto e finalità di esso; valutare i principi di necessità e proporzionalità in base alle finalità del trattamento, ed in merito vanno individuate le misure necessarie per conformarsi ai principi di cui sopra, nonché le misure necessarie per garantire i diritti degli interessati; infine la DPIA si occupa della gestione dei rischi per i diritti e le libertà degli interessati, quindi va effettuata un'analisi sui rischi, considerando le fonti di rischio, gli impatti potenziali per i diritti e le libertà delle persone qualora si verificasse l'accesso illegittimo, la modifica indesiderata dei dati e la loro perdita, la probabilità e la gravità che si verifichi la minaccia, nonché le misure previste per il trattamento di tali rischi. In merito alla Valutazione d'impatto è richiesto un parere al DPO.

Nel modello sviluppato si è tenuto conto di tutti questi elementi al fine di fornire al Titolare del trattamento uno strumento utile in termini di responsabilizzazione, in quanto funge da supporto, aiutando il Titolare a dimostrare l'adozione di misure idonee a garantire il rispetto della normativa in questione.

Questo modello è formato da quattro sezioni di carattere quantitativo-qualitativo aventi lo scopo di analizzare il trattamento minuziosamente scomponendolo in più parti. Nel corso della tesi si è fornito un'analisi approfondita delle quattro sezioni.
La prima, di carattere quantitativo, denominata Check-list, fornisce un determinato numero di adempimenti di cui il titolare del trattamento dovrà tenere conto al fine di essere conforme al Regolamento UE n. 2016/679. Per ciascun adempimento viene calcolato il rischio potenziale da parte del titolare, che dovrà dare un giudizio soggettivo sui presidi impiegati per eliminare, o almeno attenuare, il rischio potenziale effettuando i controlli adeguati.
La seconda parte, di carattere prettamente descrittivo, funge da completamento alla prima, in quanto fornisce delle informazioni aggiuntive in merito al trattamento, al fine di mettere a disposizione dei terzi un'analisi completa, trasparente e dettagliata del trattamento in

esame, rispettando il principio di trasparenza. Sempre in questa sezione compare anche il parere del Responsabile della Protezione dei Dati in merito alla DPIA, così come previsto dallo stesso GDPR e dalle Linee guida del WP29.
Per quanto riguarda la terza sezione, questa è costituita da una tabella a doppia entrata che contiene per l'appunto la "sintesi" del rischio residuo, il quale viene tramutato in scoring di rischio residuo (indice di rischio residuo) per ciascun elemento considerato, che è un numero intero ovvero: 0, 1, 2, 4, 5, in corrispondenza del quale corrisponde un giudizio, rispettivamente basso, mediamente basso, mediamente elevato, elevato e di continuità. Successivamente viene effettuata la media sull'indice di rischio residuo, per arrivare a determinare l'indice di rischio residuo medio (scoring medio) riferito all'intero trattamento e non ai singoli componenti.
Infine, l'ultima parte costituisce una specie di "diario" in cui il Titolare del trattamento annota tutte le variazioni in merito al trattamento. Questa sezione è di aiuto nella fase di monitoraggio della Valutazione d'impatto, in quanto si tratta di un processo dinamico che si evolve continuamente, va monitorata sempre.

Questo modello può essere utilizzato per trattamenti di dati in vari settori, in quanto tiene in considerazione di tutte le indicazioni fornite dal WP29 nelle Linee guida in merito allo svolgimento della DPIA, nonché delle disposizioni previste dal GDPR. Si è cercato di dimostrare la validità del modello applicandolo in vari ambiti organizzativi: come l'azienda ospedaliera, il Call Center (telemarketing), la videosorveglianza sul posto di lavoro ed infine la Banca. La sua applicabilità è possibili in tutte queste realtà perché si basa sul principio di conformità, e quindi include tutti gli adempimenti che un titolare è tenuto a perseguire per essere conforme alla normativa europea. Ovviamente ciascun Titolare sulla base della tipologia di dati trattati, delle finalità del trattamento, del contesto e della natura del trattamento, valuterà il rischio inerente al trattamento stesso, e provvederà alla gestione della tipologia di rischio, allo scopo di attenuarlo attraverso l'impiego degli strumenti organizzativi e tecnologici a disposizione fino a raggiungere un livello di rischio residuo accettabile.

Bibliografia

1. Altman, I., 1975. The environment and social behavior: Pryvacy, personl space, territory, crowding. Montrey: Brooks/Cole Pub. Co..
2. Arendt, H., 1948. Le origini del totalitarismo. Torino: Piccola biblioteca Einaudi.
3. Arendt, H., 1964. Vita activa. La condizione umana. Milano: Bompiani.
4. Ariès, P., 1988. La vita privata. s.l.:Laterza.
5. Aristotele, 1981. La Politica. Firenze: Le Monnier.
6. Austin, J., 1873. Lectures on Jurisprudence. IV ed. London: Albemarle Street.
7. Bellazzi, M., 2003. I "Patriot Acts" e la limitazione dei diritti costituzionali negli Stati Uniti. Politica del Diritto, XXXIV(4), pp. 681-706.
8. Brandeis, L. D., 1928. dissenting opinion in Olmstead vs. U.S.. s.l.:s.n.
9. Cafari Panico R., 2013. Da internet ai social network. s.l.:Maggioli Editore.
10. Castells, M., 2002. Galassia Internet. Milano : Feltrinelli.
11. Cooper, J., 1838. The american democrat, Ed. Barnes Noble Books, 2004. I ed. New York: The american democrat, Ed. Barnes Noble Books, 2004.
12. De Tocqueville, A., 1989. l'antico regime e la rivoluzione. Milano: Rizzoli.
13. Faulkner, W., 1955. Privacy. Il sogno americano: che cosa né è stato? Milano: Piccola Biblioteca Adelphi.
14. Fumagalli Meraviglia, M., 2016. Le nuove normative europee sulla protezione dei dati personali. Diritto comunitario e degli scambi internazionali.
15. Fuster, G. G., 2014. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Dordrecht: Springer.
16. Galgani, F., 23 luglio 2014.La nascita del diritto alla privacy negli Stati Uniti e Europa, in Informatica libera - blog di Francesco Galgani.
17. Garante per la protezione dei dati personali - Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e delle libertà fondamentali; (CEDU)
18. Garante per la protezione dei dati personali - Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale; (n.108)

19. Garante per la protezione dei dati personali - Direttiva 95/46/CE del Parlamento e del Consiglio europeo “relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati”.

20. Garante per la protezione dei dati personali - Gruppo di Lavoro Articolo 29, parere n. 3/2010 “sul principio di responsabilizzazione”.

21. Garante per la protezione dei dati personali - Linee guida in materia di valutazione d’impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679, adottate il 4 aprile 2017 come modificate e adottate da ultimo il 4 ottobre 2017;

22. Garante per la protezione dei dati personali - Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016 (Versione emendata e adottata in data 5 aprile 2017);

23. Garante per la protezione dei dati personali, 2016. Guida allapplicazione del Regolamento europeo in materia di protezione dei dati personali.

24. Gazzetta Ufficiale dell’Unione europea, 2016, Rettifica del 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) (GU L 119 del 4.5.2016).

25. Gazzetta Ufficiale della Repubblica Italiana- D. Lgs. 10 agosto 2018, n. 101 recante “Disposizioni per l’adeguamento della normativa nazionale alle disposizioni del 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)”.

26. Gazzetta Ufficiale della Repubblica Italiana, 2016, Legge n.300/1970 modificata successivamente al Parere espresso dal Ministero del Lavoro e delle Politiche sociali dal D. Lgs. 24 settembre 2016, n.185.

27. Gazzetta Ufficiale della Repubblica italiana, 2018, legge 11 gennaio 2018, n. 5, recante disposizioni in materia di iscrizione e funzionamento del registro delle opposizioni e istituzione di prefissi nazionali per le chiamate telefoniche a scopo statistico, promozionale e di ricerche di mercato, entrata in vigore il 4 febbraio 2018;

28. Gianniti, P., 2015. La CEDU e il ruolo delle corti. Bologna: Zanichelli.

29. Glancy, D., 1979. The invention of the right to privacy. Arizona Law Review, 21.

30. Handlin, O., 1964. Out of many: a study guide to cultural pluralism in the United States. Anti-defamation League of B'nai B'rith.

31. Hondius, F. W., 1975. Emerging data protection in Europe. Amsterdam: North-Holland Publishing. Hosein, Rouvroy Poullet, 2009. Reinventing Data Protection?. s.l.:Springer.

32. Iaselli, M. e Gorla, S., 2015. Storia della Privacy. Roma: Edizione Lex Et Ars.

33. Lamendola, F., 2013. L'Individualismo Assoluto della modernità è qualcosa di anti-umano. Arianna Editrice, 29 Aprile.

34. Locke, J., 1690. Due trattati sul governo. s.l.:Plus Edizioni.

35. Maletta, S., 1999. Il totalitarismo come forma di pensiero. La Nuova Europa, Issue 6, pp. 78-86.

36. Marescotti, D., 2005. I totalitarismi del XX secolo e la manipolazione delle coscienze. Peacelink, 20 Marzo.

37. Mariani, G. S., Reposo, A. Patrono, M., 1999. Guida alla Costituzione degli Stati Uniti d'America. IV ed. Milano: Rizzoli.

38. Miglietti, L., 2014. Profili storico comparativi del diritto alla privacy. In Diritti comparati. [Online]

39. Miller, P., 1965. The Life of the Mind in America: From the Revolution to the Civil War. I ed. s.l.:Harcourt.

40. Modafferi, F., 2015. Lezioni di diritto alla protezione dei dati. s.l.:lulu.com.

41. Mumford, L., 1954. La Cultura delle Città. Milano: Edizioni di Comunità.

42. Niger, S., 2006. Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali. Padova: Cedam.

43. Pizzetti, F. M., 2016. Privacy e il diritto europeo alla protezione dei dati personali. Torino: G. Giappichelli Editore.

44. Platone, 2007. La Repubblica. Roma: Armando Editore.

45. Rodotà, S., 1974. La privacy tra individuo e collettività, in Politica del diritto, 1974. Bologna: Il Mulino.

46. Rodotà, S., 2006. La vita e le regole: tra diritto e non diritto. Milano: Feltrinelli Editore.

47. Rodotà, S., 2014. Il mondo nella rete. Quali i diritti, quali i vincoli. Roma: Laterza.

48. Rosen, J., 2001. The unwanted gaze: The destruction of privacy in America. New York: Vintage Books.

49. Sacerdoti Mariani, G., Reposo, A. Patrono, M., 1999. Guida alla Costituzione degli Stati Uniti d'America. Milano: Sansoni.

50. Saetta B., 19 maggio 2018. Convenzione 108 del Consiglio d'Europa. [Online]

51. Shirer, W., 1960. The Rise and Fall of the Third Reich. Torino: Einaudi.

52. Smith R. E., 2000. Ben Franklin's website: Privacy and curiosoty from Plymouth Rock to the Internet. Privacy Journal.

53. Soffientini, M., 2018. Privacy - protezione e trattamento dei dati.Ipsoa Manuali. Assago: Wolters Kluwer.

54. Swire, P. Berman, S., 2007. Information Privacy. s.l.:IAPP Publication.

55. Testi, A., 2013. Short Cuts America: il blog di Arnaldo Testi. [Online]

56. Ufficio delle pubblicazioni dell'Unione europea, 2018, Manuale sul diritto europeo in materia di protezione dei dati edizione 2018, Lussemburgo.

57. Warren, S. Brandeis, L., 1890. The Right to Privacy, in Harvard Law Review , Volume 4.

58. Westin, A. F., 1967. Privacy and Freedom. New York: Atheneum.

59. Whitman, J. Q., 2004. The Two Western Cultures of Privacy: Dignity Versus Liberty. The Yale law journal, 113(6).

Ringraziamenti

In primis, vorrei ringraziare la mia famiglia, che mi ha sempre incoraggiata, aiutata e ha sempre creduto in me, anche quando io stessa pensavo di non farcela più. Siete la mia ancora di salvezza in un mare in tempesta, il barlume di luce dentro un tunnel, il mio tutto!

Un grazie di cuore va ai miei genitori che ci sono sempre ad aiutarmi e a sostenermi, a dare tutto loro stessi solo per vedermi felice e realizzata, senza di loro sarei completa solo a metà.

Un grazie speciale va alla migliore sorella del mondo, sulla quale potrò sempre contare.

Vorrei inoltre ringraziare le mie amiche e i miei amici per la comprensione e i momenti felici passati insieme.

In particolare vorrei ringraziare il Professore Simone Mazzonetto per avermi accompagnata in questo percorso che segna la fine della mia carriera universitaria.

Infine, un grazie va a me stessa, per non aver mollato nonostante tutte le difficoltà. L'ambizione fa la differenza.