ALESSIO
LIVI

TTS
CENTRO STUDI SVILUPPO
RELAZIONI PER LA SICUREZZA

LA RESPONSABILITÀ CIVILE DA ILLECITO TRATTAMENTO DEI DATI PERSONALI

Alessio Livi autore

La responsabilità civile da illecito trattamento dei dati personali

ISBN: **9791281687035**

Realizzato e pubblicato in collaborazione con l'autore da

Centro Studi Sviluppo Relazioni per la Sicurezza – TTS

Università degli studi di Roma UnitelmaSapienza

Sito intennet: www.ttsecurity.it

E-mailcentrostuditts@gmail.com

Instagram: Tts Centrostuditts
Facebook: TTS Centro Studi Sviluppo Relazioni per la Sicurezza
Linkedin: TTS thinktanksecurity
YouTube: Centrostudi TTS

Alessio Livi

La responsabilità civile da illecito trattamento dei dati personali

Raggiungere un importante risultato,

ripaga molto più di entusiasmanti motivi per non averlo fatto!

Note

Per esigenze personali e per permettere una più facile lettura a persone con DSA[1] di tipo dislessia[2], il presente elaborato è stato realizzato secondo i criteri "ad alta leggibilità" in base alle linee guida sulla gestione dei Disturbi Specifici dell'Apprendimento dell'Associazione Italiana Dislessia[3].

1. **Carattere:**
   - tipo di carattere Verdana;
   - dimensione carattere 12;
   - interlinea e spaziatura paragrafo 1,5.
2. **Mappe concettuali:**
   - al termine di ogni capitolo e/o paragrafo contenente elementi salienti, è stata realizzata una mappa concettuale aggiuntiva; al riguardo di seguito è presente un indice della didascalia.

[1] I Disturbi Specifici dell'Apprendimento (DSA) sono: 1) Dislessia (disturbo specifico della lettura); 2) Disortografia (disturbo specifico della scrittura); 3) Disgrafia (disturbo specifico della grafia); 4) Discalculia (disturbo specifico nella manipolazione dei numeri). Essi riguardano il neuro-sviluppo con implicazioni della capacità di leggere, scrivere agilmente e di calcolare in modo corretto e fluente. Sono disordini che dipendono dalle diverse modalità di funzionamento delle reti neuronali coinvolte nei processi di lettura, scrittura e calcolo, cioè da un diverso funzionamento del cervello e delle sue modalità di apprendimento. I DSA non sono una malattia, non sono causati da un deficit di intelligenza, né da problemi ambientali o psicologici e nemmeno da deficit sensoriali. https://www.aiditalia.org/che-cosa-sono-i-dsa

[2] I principali dati relativi agli studenti con DSA: Dislessia (pari al 39,6%); 2) Disortografia (pari al 21,5%); 3) Disgrafia (pari al 18,6%); 4) Discalculia (pari al 20,3%) - I principali dati relativi agli alunni con DSA, Novembre 2020, Ministero dell'Istruzione e del Merito

[3] Associazione Italiana Dislessia www.aiditalia.org

Indice

Note 2

Indice 3

Abstract 6

Capitolo Primo - Premessa 7

Il contesto normativo generale di riferimento 9

Capitolo Secondo - La storia del diritto alla privacy 14

Le origini nel mondo, in Europa e in Italia 14

Origini e sviluppo del diritto alla privacy, il riconoscimento giuridico negli Stati Uniti 14

L'evoluzione del concetto di privacy in Europa: un percorso giuridico lungo e complesso 20

Il diritto alla riservatezza in Italia 28

Dalla privacy alla protezione dei dati personali 32

L'era dell'Information and Communication Technologies (ICT) 39

L'equilibrio fra diritti fondamentali e libera circolazione delle informazioni 44

Capitolo Terzo - L'accountability 55

Il principio generale 55

L'accountability nel GDPR 56

Capitolo Quarto - La responsabilità civile da illecito trattamento dei dati personali 65

La tutela rimediale 65

La tutela in autonomia 69

La tutela amministrativa 69
La tutela giurisdizionale 70
Il Profilo soggettivo 74
La legittimazione attiva 74
La legittimazione passiva e le nuove figure tipiche 76
Il titolare del trattamento 78
I contitolari del trattamento 79
Il responsabile del trattamento, la sub-responsabilità e co-responsabilità..... 80
Il rappresentante del titolare o del responsabile..... 85
Il Responsabile della protezione dei dati – DPO (Data Protection Officer) 85
Il Profilo oggettivo..... 88
I principi fondamentali del trattamento dei dati personali 88
La responsabilità per trattamento illecito 100
Il danno 102
Il criterio di imputazione..... 111
Conclusioni 115
Il panorama del GDPR e il principio dell'accountability..... 115
Responsabilità e risarcimento per violazioni del GDPR 115
Prospettive future: l'influenza del GDPR 117
La sfida globale..... 120
Bibliografia 121
Ringraziamenti 123

Didascalia

Mappa concettuale 1 – Il contesto normativo generale di riferimento 13
Mappa concettuale 2 – Evoluzione del Diritto alla Privacy negli USA .. 19
Mappa concettuale 3 – Evoluzione del diritto alla Privacy in Europa ... 27
Mappa concettuale 4 - Il diritto alla riservatezza in Italia 38
Mappa concettuale 5 – L'era dell'ICT 43
Mappa concettuale 6 – L'equilibrio fra diritti fondamentali e libera circolazione delle informazioni 54
Mappa concettuale 7 – L'accountability 64
Mappa concettuale 8 – La tutela rimediale privatistica 73
Mappa concettuale 9 - Il Responsabile del trattamento 84
Mappa concettuale 10 - Il profilo soggettivo 87
Mappa concettuale 11 - I principi fondamentali del trattamento dei dati personali 99
Mappa concettuale 12 – Il danno 114

Abstract

La tesi affronta il contesto normativo del diritto alla privacy partendo dalla sua nascita, con particolare attenzione al riconoscimento giuridico negli Stati Uniti e al percorso in Europa ed in Italia, e prosegue con l'analisi della sua evoluzione sino alla transizione verso il nuovo diritto alla protezione dei dati personali, attraverso la nuova era dell'Information and Communication Technologies, esaminando l'equilibrio tra diritti fondamentali e libera circolazione delle informazioni. Un'attenzione particolare è dedicata al principio dell'accountability, introdotto dal Regolamento Generale sulla Protezione dei Dati. La tesi affronta poi il tema della responsabilità civile derivante dal trattamento illecito dei dati personali, con l'analisi delle diverse forme di tutela rimediale, dei profili di legittimazione attiva e passiva, studiando le nuove figure coinvolte nel trattamento dei dati. L'elaborato esplora inoltre i requisiti oggettivi della responsabilità da illecito trattamento dei dati e, anche attraverso l'analisi della giurisprudenza, analizza i principi fondamentali del trattamento dei dati personali, il concetto di danno ed il criterio d'imputazione, evidenziando il collegamento con il principio di responsabilizzazione.

The dissertation delves into the regulatory landscape of the right to privacy, commencing from its inception, with a focused exploration of its legal recognition in the United States and its trajectory within Europe and Italy. It progresses by analysing its evolution towards the transition to the new right to safeguard personal data, amidst the Information and Communication Technologies era, whilst examining the equilibrium between fundamental rights and the unimpeded circulation of information. Particular attention is directed towards the principle of accountability, as introduced by the General Data Protection Regulation. The dissertation further addresses the theme of civil liability arising from the wrongful handling of personal data, encompassing an analysis of various forms of remedial safeguards, active and passive legitimacy profiles, and a study of the novel stakeholders engaged in data processing. Additionally, the paper explores the objective criteria for liability due to illicit data processing and, through a scrutiny of legal precedents, dissects the fundamental tenets of personal data handling, the concept of harm, and the criterion of attribution, emphasising the correlation with the principle of accountability.

Capitolo Primo - Premessa

Nel panorama giuridico moderno, il dibattito dottrinale ha ampiamente affrontato la complessa questione della responsabilità civile inerente al trattamento illecito dei dati personali. La questione, infatti, verrà esaminata alla luce dell'evoluzione legislativa intervenuta in materia a partire dalla Legge 31 dicembre 1996, n. 675[4], che rappresentò il primo atto normativo italiano mirato a delineare in modo sistematico la protezione della riservatezza e dei dati personali. Un passaggio successivo di cruciale rilievo è stato rappresentato dal Decreto Legislativo del 30 giugno 2003, n. 196[5], noto come "*Codice della Privacy*", che ha ulteriormente forgiato il quadro giuridico in materia.

L'elaborato si focalizza sull'analisi della particolare disciplina giuridica concernente la responsabilità civile derivante dal trattamento illecito dei dati personali. Tale disciplina è oggetto di un'analisi inquadrata nel contesto della mutata dinamica legale sottesa al nuovo principio della responsabilizzazione, noto anche come "*accountability*", che rappresenta un aspetto di rilievo nell'attuale panorama giuridico, e pertanto si presta a essere esaminato con dettaglio. L'attenzione è rivolta in particolar modo ai nodi problematici inerenti alla natura del danno derivante dall'illecito trattamento dei dati, alla ricomparsa del danno non patrimoniale ed alla sua risarcibilità.

In un contesto sociale ed economico reso complesso dall'accelerato avanzamento tecnologico, l'intersezione tra diritto e tecnologia ha dato vita a un nuovo scenario legale e sociale, con relativo conseguente dibattito. Questo scenario è caratterizzato da un intreccio inedito di interazioni tra individui, organizzazioni e flussi di informazioni. In tale quadro, i dati personali hanno assunto un ruolo centrale e sono divenuti una sorta di valuta digitale, con un valore intrinseco che permea ogni settore dell'attività umana.

[4] Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

[5] Decreto Legislativo n. 196 del 30 giugno 2003 - Codice in materia di protezione dei dati personali.

Da questa evoluzione emerge un interrogativo cruciale: come bilanciare l'impulso innovativo dell'era tecnologica con l'esigenza irrinunciabile di proteggere i diritti fondamentali degli individui? In questo contesto, il diritto alla privacy e la tutela dei dati personali si pongono come pilastri fondamentali, i quali dettano l'equilibrio tra progresso tecnologico e tutela dei diritti umani.
La presente tesi si prefigge l'obiettivo di esplorare le varie sfaccettature connesse alla complessa questione della responsabilità civile per illecito trattamento dei dati personali.
La trattazione si avvia con l'analisi della storia del diritto alla privacy nei vari periodi: si parte dall'origine di tale diritto per poi analizzare le prime forme di evoluzione verso la tutela dei dati personali, attraversando le fasi iniziali dell'età moderna per giungere infine ai nostri giorni. Verranno condotti approfondimenti sulle evoluzioni e declinazioni di principi e norme, a livello internazionale, europeo ed italiano. Ci si concentrerà poi sul concetto di responsabilizzazione (accountability), che costituisce un principio cardine nella gestione e protezione dei dati personali. Un esame delle Direttive europee[6] e dei principi stabiliti dal Regolamento europeo[7] UE 2016/679, il Regolamento Generale per la Protezione dei Dati Personali - RGPD, in inglese e più comunemente noto come GDPR - General Data Protection Regulation (d'ora in avanti denominato GDPR o anche Regolamento)[8], consentirà di comprenderne l'implicazione nella ridefinizione

[6] La Direttiva europea è un atto tipico, fonte di diritto derivato, di portata generale, obbligatorio, tuttavia privo della qualità della diretta applicabilità. È quindi previsto l'intervento degli Stati membri destinatari dell'atto che dovranno adottarlo/recepirlo, ma -si badi- solo con riguardo al risultato da raggiungere, ovvero nella piena libertà di scelta dei mezzi e della forma.
[7] Il Regolamento europeo è un atto tipico, fonte di diritto derivato, di portata generale, obbligatorio e di diretta applicabilità. Ciò implica che esso entri in vigore nei singoli Stati membri senza richiedere ulteriori provvedimenti di adozione, recepimento o adattamento da parte dei rispettivi sistemi giuridici (le disposizioni del Regolamento sono dunque self-executing), salvo specifici casi, come per il GDPR.
[8] Regolamento UE 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 General Data Protection Regulation (GDPR, EU RGPD), 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 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela

delle pratiche di raccolta, elaborazione e conservazione dei dati personali. L'abbandono di un approccio formale a favore di una cultura basata su trasparenza, responsabilità e dimostrabilità della conformità alle norme, sarà oggetto di approfondimento ed analisi critica.
La parte centrale della tesi sarà dedicata all'analisi della responsabilità civile insorgente dall'illecito trattamento dei dati personali. Si analizzeranno i diversi rimedi e ci si soffermerà sull'indagine dei concetti di danno ingiusto e danno non patrimoniale, analizzati alla luce del quadro normativo e delle giurisprudenze europea e nazionale.

Il contesto normativo generale di riferimento

Come anticipato, il presente elaborato si propone di approfondire le questioni inerenti al trattamento illecito dei dati, alla correlata responsabilità e al conseguente danno (con una particolare attenzione al danno non patrimoniale), all'interno del contesto normativo articolato europeo e italiano. Questo quadro giuridico integrato è delineato da due pilastri fondamentali: da un lato, il noto sopracitato Regolamento Generale per la Protezione dei Dati Personali (GDPR), il quale si applica dal 25 maggio 2018; dall'altro, il processo di standardizzazione guidato dal Decreto Legislativo 101/2018[9], entrato in vigore il 19 settembre 2018, che ha rimodellato il preesistente Decreto Legislativo 196/2003, noto come Codice della Privacy, trasformandolo nel "*Nuovo Codice della Privacy*".
Il GDPR e il Nuovo Codice della Privacy costituiscono le basi su cui si fonda l'analisi giuridica oggetto del presente studio. Tuttavia, è importante evidenziare

delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

[9] Decreto Legislativo, n. 101 del 10 agosto 2018 - 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 del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

che le norme in materia di responsabilità sono contenute nel GDPR e non, invece, nel Nuovo Codice della Privacy, che precedentemente rappresentava il riferimento generale per la responsabilità legata al trattamento illecito dei dati personali.

L'articolo 1 del GDPR stabilisce l'introduzione di norme atte a proteggere i dati personali e a garantire la libera circolazione degli stessi, assicurando la tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. L'ambito di applicazione soggettivo del GDPR è circoscritto alle persone fisiche, con una specifica eccezione per i dati personali delle persone decedute. Gli Stati membri possono stabilire norme riguardanti il trattamento dei dati personali di persone decedute.

Il GDPR, nel delineare i diritti di protezione dei dati personali, esclude dal suo campo di applicazione i trattamenti effettuati da persone fisiche per attività esclusivamente personali o domestiche.

Un ulteriore elemento di rilievo è l'attenzione posta nei Considerando del GDPR sulla definizione di informazioni anonime, le quali non rientrano nell'ambito di applicazione del Regolamento. Questa definizione diventa significativa nell'era digitale, dove i dati anonimi e il loro utilizzo statistico o di ricerca rappresentano una sfida da affrontare.

L'economia moderna è intrisa di tecnologia, così come lo è oggi la Pubblica Amministrazione (d'ora in avanti PA), all'interno della quale è da anni in corso un processo di ammodernamento e di così detta digitalizzazione[10]. Oggi, dunque, si parla sempre più spesso di trasformazione digitale della PA[11] e di

[10] Digitalizzazione: la conversione di grandezze analogiche in informazioni digitali, Enciclopedia on line Treccani https://www.treccani.it/enciclopedia/digitalizzazione/

[11] La trasformazione digitale della Pubblica Amministrazione (PA) si prefigge di cambiare l'architettura e le modalità di interconnessione tra le basi dati delle amministrazioni. Avere banche dati pubbliche che parlano tra loro, contribuisce a un risparmio economico, per le amministrazioni, e di tempo, per i cittadini, Dipartimento per la trasformazione digitale https://innovazione.gov.it/italia-digitale-2026/il-piano/digitalizzazione-della-pa/

dematerializzazione della documentazione cartacea[12]; tutto ciò influenza sia la sfera produttiva che quella personale di ogni cittadino. L'intenso utilizzo dei dati, insito nella digitalizzazione, ha portato a considerare l'informazione come la chiave per lo sviluppo economico:

> "*Il risparmio di risorse ottenuto può essere impiegato per investimenti o impieghi alternativi, e la digitalizzazione della Pubblica Amministrazione viene a essere quindi un motore per lo sviluppo economico.*"[13]

Questa digitalizzazione ha però innescato una tensione tra la tutela dei diritti fondamentali delle persone e la libertà del mercato, soprattutto nei settori digitali. Tuttavia, la corretta lettura del quadro normativo, orientata alla costituzione e ai diritti fondamentali, dimostra che questa tensione non può minare la protezione dei diritti umani.

La Commissione europea[14] (Commissione Ue) ha affrontato la sfida della tutela della privacy e dei dati personali attraverso l'approvazione del GDPR; tuttavia, rimane ancora da completare il quadro normativo con la scrittura del tassello cruciale della privacy digitale, ovvero quello riguardante la circolazione dei dati personali nelle comunicazioni digitali dovute alle recenti innovazioni rappresentate principalmente dall'Internet of Things (IoT, internet delle cose,

[12] La dematerializzazione della documentazione amministrativa https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo/libro_bianco_dematerializzazione.pdf

[13] DigitPA, Ente nazionale per la digitalizzazione della Pubblica Amministrazione, Dizionario di Economia e Finanza Treccani https://www.treccani.it/enciclopedia/digitpa_%28Dizionario-di-Economia-e-Finanza%29/

[14] La Commissione europea detiene il potere esecutivo nell'interesse generale dell'Unione Europea (UE) e promuove l'iniziativa legislativa al suo interno. Ha inoltre il compito di vigilare sull'osservanza delle Norme di diritto primario (il TUE - Trattato sull'Unione Europea, il TFUE - Trattato sul Funzionamento dell'Unione Europea e i relativi Protocolli ed Allegati) e di diritto derivato (gli Atti Tipici, come Regolamenti, Direttive e Decisioni) attraverso la procedura di infrazione, oltre che di tutelare il rispetto dei valori dell'Unione attraverso la procedura di accertamento e sanzione. https://commission.europa.eu/index_it

come ad esempio, smartphone, frigoriferi intelligenti, smartwatch, assistenti virtuali come Alexa, Google Home, ecc.)[15].

Al riguardo è in corso la riforma della Direttiva 2002/58/CE[16], che mirava già 20 anni fa a disciplinare il tema dell'innovazione Information and Communication Technologies (d'ora in avanti ICT), con l'obiettivo di aggiornare e soprattutto uniformare[17] il quadro normativo europeo.

In Italia, come anticipato, le regole per la protezione dei dati personali sono state introdotte per la prima volta attraverso la Legge 31 dicembre 1996, n. 675, che successivamente è stata sostituita dal Codice in materia di protezione dei dati personali (il già citato Decreto Legislativo 196/2003), noto come Codice Privacy. Questo Codice è stato ampiamente rivisto attraverso il sopracitato Decreto Legislativo del 10 agosto 2018, n. 101, in risposta alla piena applicazione del GDPR. Tale intervento normativo, col chiaro fine di "*armonizzazione*", ha inoltre abrogato espressamente alcune parti obsolete ed ormai incompatibili con il GDPR.

In altre parole, il quadro normativo in materia di dati personali è costituito sia dal GDPR europeo sia dal Nuovo Codice della Privacy italiano, in un continuo tentativo di entrambi i legislatori di trovare un equilibrio tra le esigenze dell'era digitale e la tutela dei diritti fondamentali delle persone. La tensione tra questi obiettivi viene affrontata attraverso una visione costituzionalmente orientata, che ricerca un punto d'incontro tra la tutela dei dati personali e la libertà economica.

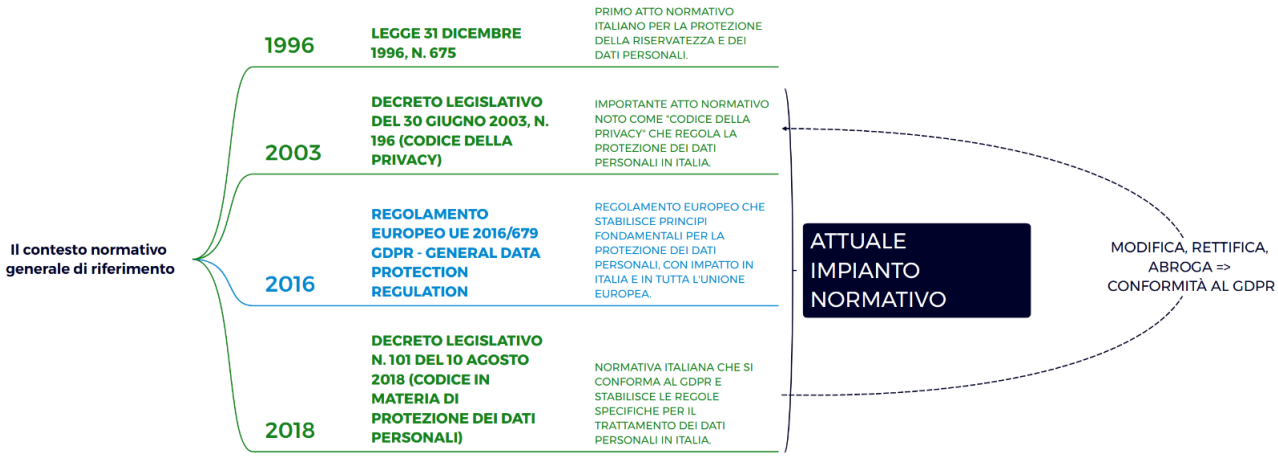
---

[15] Internet of Things: tecnologie hardware e software che dispongono di sensori e altre tecnologie integrate allo scopo di connettere e scambiare dati, anche personali, con altri dispositivi e sistemi su Internet https://www.garanteprivacy.it/temi/iot, https://www.oracle.com/it/internet-of-things/what-is-iot/

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

[17] Per armonizzazione s'intende il procedimento finalizzato all'incremento del grado di coerenza ed armonia tra normative e regolamenti diversi, mirando al conseguimento di un accordo sostanziale tra di essi, dunque di conformità. Dall'altro lato, la "standardizzazione" rappresenta il procedimento per mezzo del quale norme e regolamenti vengono amalgamati ed unificati, con l'obiettivo di stabilire l'uniformità tra di essi.

Mappa concettuale 1 – Il contesto normativo generale di riferimento



Capitolo Secondo - La storia del diritto alla privacy

Le origini nel mondo, in Europa e in Italia

Origini e sviluppo del diritto alla privacy, il riconoscimento giuridico negli Stati Uniti

Nel panorama dei diritti della personalità, il diritto alla privacy non può vantare il titolo di "primogenito". Per lungo tempo relegato nell'ombra, esso ha subito un graduale processo evolutivo che ha alterato sia la sua struttura che il suo contenuto. Nel corso di tale mutamento, il diritto alla privacy è stato sempre più frequentemente invocato al fine di proteggere interessi già presidiati da altri diritti riconosciuti a vantaggio dell'individuo. In tal modo, il diritto in questione ha assunto una posizione preminente, divenendo uno dei mezzi di tutela personale di maggiore rilievo.

La gran parte della formulazione del diritto alla privacy è attribuibile all'esperienza statunitense alla fine del 1800. Inizialmente, questo diritto non trovò menzione esplicita in alcuna normativa giuridica positiva, ma fu plasmato e sviluppato attraverso il progresso delle interpretazioni giurisprudenziali. Il termine "*privacy*" trova origine in un articolo pubblicato nella Harvard Law Review oltre un secolo fa (nel 1890), intitolato "*The Right to Privacy*"[18]. Tale articolo riguardava la vita di Samuel D. Warren, un brillante giovane avvocato di Boston. Questi sviluppò una crescente avversione nei confronti delle intrusioni dei media nella sua sfera privata, in particolare quando un giornale di Boston cominciò a dedicare molta attenzione al suo stile di vita, particolarmente mondano dopo il suo matrimonio con la figlia di un influente politico, il senatore Bayard. Infastidito dall'eccessiva esposizione della sua vita privata, Warren, insieme al suo compagno di studi universitari Louis D. Brandeis, decise di

[18] The Right to Privacy, Samuel D. Warren, Louis D. Brandeis, Boston - USA, Dicembre 1890
https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

denunciare questa invadenza dei media nella sfera personale. Nell'articolo che scrissero per affrontare questo problema, sottolinearono che, così come un individuo ha il diritto di difendere la sua proprietà, ha anche il diritto di proteggere la sua intimità e solitudine. In tal senso, suggerirono l'idea di introdurre un nuovo concetto giuridico, un nuovo illecito specifico, per contrastare tali intrusioni.

Il saggio, inoltre, esaminava la questione delle innovazioni tecnologiche dell'epoca, come la stampa a rotativa, la diffusione dei giornali e l'invenzione della fotografia istantanea. Questi strumenti si profilavano come potenziali mezzi capaci di generare nuove forme di violazione dei diritti individuali.

Questo processo contribuì a gettare le fondamenta per la attuale concezione del diritto alla privacy, così come disciplinato nelle prime normative internazionali di tutela.

Il descritto contesto storico è dunque quello degli Stati Uniti d'America della fine del XIX secolo, un periodo di rapida evoluzione tecnologica e sociale. La storia del riconoscimento giuridico del concetto di privacy negli Stati Uniti è stata successivamente segnata da una serie di sviluppi che hanno fornito le basi per il futuro dibattito sulla questione della riservatezza. Nel 1927, in occasione del procedimento giudiziario Olmstead vs. United States[19], emerse la questione della legittimità delle intercettazioni telefoniche svolte da agenti dell'FBI senza previo mandato giudiziario. Tale contesto giuridico costituì una tappa rilevante nel dibattito.

Successivamente, nel 1934, il Congresso introdusse un sistema di regolamentazione per la sorveglianza elettronica e approvò il Communication Act[20]. La sezione 605 di questa legge proibiva l'intercettazione delle

[19] Il caso Olmstead contro gli Stati Uniti del 1927 si è rivelato incredibilmente importante e influente. Il caso ruotava attorno all'accusa di Roy Olmstead, residente nello stato di Washington, di aver tentato di contrabbandare e vendere alcolici in violazione del proibizionismo https://billofrightsinstitute.org/e-lessons/olmstead-v-united-states-1927

[20] The communications act of 1934, National Security Agency, USA https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/reports-research/folder_047/41786769082578.pdf

conversazioni protette dalla legge e la divulgazione del loro contenuto senza adeguata autorizzazione.

Nel 1966 il Freedom of Information Act[21] per la prima volta conferì ai cittadini il "diritto di accedere alle informazioni" detenute dalle autorità federali, rendendo disponibili la maggior parte dei documenti, archivi e dati raccolti dalle agenzie governative, con alcune eccezioni.

Un altro momento cruciale nell'affermazione di un autonomo diritto alla privacy fu rappresentato dalla causa Katz vs. United States del 1967[22]. In questa circostanza, ancora una volta, il tema centrale del processo riguardava la registrazione delle conversazioni di Charles Katz da parte degli agenti dell'FBI.

I casi giuridici Warren, Olmstead e Katz costituirono i pilastri sui quali si fondò la futura protezione del diritto alla privacy, che si concretizzò nei tardi anni '60 del XX secolo.

Nel 1974, è stato introdotto il Privacy Act[23], che ha influenzato il Freedom of Information Act (FOIA) in due modi chiave: ha limitato la divulgazione di informazioni sulla privacy dei cittadini e ha rinforzato il "diritto di essere informati" per le persone sotto indagine.

Nel 1986, è stato introdotto l'l'Electronic Communications Privacy Act (ECPA)[24], che ancora oggi assicura la tutela delle comunicazioni elettroniche dei cittadini.

---

[21] Il Freedom of Information Act (FoIA), diffuso oggi in oltre 100 paesi al mondo, garantisce a chiunque il diritto di accesso alle informazioni detenute dalle pubbliche amministrazioni, salvo i limiti a tutela degli interessi pubblici e privati stabiliti dalla legge
https://foia.gov.it/normativa/cose-il-foia

[22] Nel caso Katz contro gli USA n. 389 del 1967 la Corte Suprema degli Stati Uniti ha emesso una sentenza storica, declinando in modo innovativo il diritto alla privacy in relazione alle intrusioni immateriali che la tecnologia stava iniziando a consentire
https://supreme.justia.com/cases/federal/us/389/347/

[23] Il Privacy Act del 1974 stabilisce un codice di pratiche eque in materia di informazioni che regolamenta la raccolta, la conservazione, l'uso e la divulgazione di informazioni sugli individui mantenute nei sistemi di registrazione da parte delle agenzie federali. Un sistema di registrazione è un insieme di registrazioni sotto il controllo di un'agenzia da cui le informazioni sono recuperate mediante il nome dell'individuo o attraverso un identificatore assegnato all'individuo.

[24] L'Electronic Communications Privacy Act (ECPA), protegge le comunicazioni telematiche mentre vengono effettuate, mentre sono in transito e quando sono memorizzate su computer. La legge si applica a e-mail, conversazioni telefoniche e dati memorizzati in formato elettronico.

Sebbene sia merito di Warren e Brandeis aver tentato di dimostrare l'esistenza di un diritto alla privacy nel sistema di Common Law[25] attraverso il loro celebre articolo, il concetto del nuovo diritto "di essere lasciati soli". ("*right to be let alone*") non suscitò grande interesse. Solo a partire dagli anni '60, quando un altro giurista di nome Dean William Prosser, in un saggio pubblicato sulla California Law Review, ha razionalizzato il concetto di "Privacy" e la sua declinazione attraverso quattro categorie distinte[26], ha permesso che il tema uscisse dall'angolo in cui era stato confinato, assumendo un ruolo centrale nel dibattito giuridico statunitense.

Successivamente, come accennato in precedenza, fu principalmente la giurisprudenza, coadiuvata dal lavoro svolto dalla dottrina, a definire i passi evolutivi della tutela della privacy. Tuttavia, fino alla metà degli anni '60, le corti statunitensi riconoscevano la tutela della vita privata principalmente quando strettamente correlata al diritto di proprietà.

Solo a partire dal 1965, con il caso Griswold v. Connecticut, si iniziò a riconoscere il concetto di privacy come qualcosa di distinto dal diritto di proprietà, vedendolo invece come espressione della libertà di autodeterminazione.

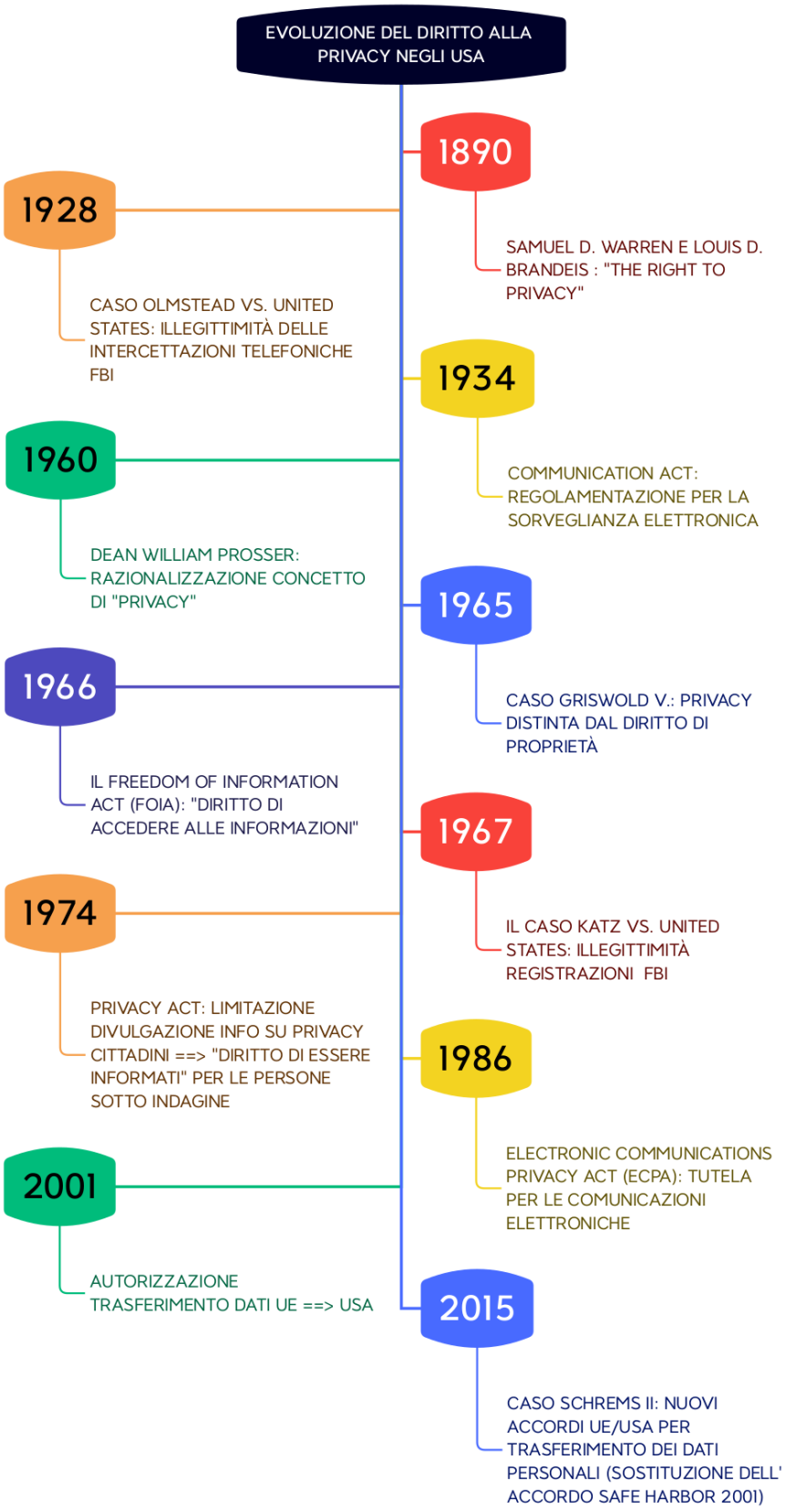
Questa prospettiva si sviluppò ulteriormente, creando una netta distinzione tra il concetto di privacy come sinonimo di autonomia decisionale e sviluppo personale, e il concetto di privacy come ricerca di solitudine e riservatezza, tipici dell'individuo. Come esamineremo in dettaglio in seguito, questa nuova dimensione in cui si inquadra la privacy rappresentò un punto di svolta nel dibattito, passando dal "diritto di essere lasciati soli" a una dimensione più

[25] Sistema giuridico inglese (e dei paesi anglosassoni, in genere) sviluppatosi ad opera delle Corti regie di giustizia. La struttura giuridica elaborata dalle Corti è profondamente diversa da quella di tradizione romanistica. Il Common Law si è sviluppato essenzialmente come diritto giurisprudenziale, per cui sono gli stessi giudici, attraverso le loro pronunce, a creare il diritto, vincolando anche le decisioni giurisprudenziali successive (cd. case laws). Caratteristico dei sistemi di Common Law è l'inesistenza della tradizionale partizione romanistica tra diritto privato e diritto pubblico. Dizionari Simone https://dizionari.simone.it/1/common-law

[26] 1) entrare in uno spazio privato; 2) divulgare fatti privati in pubblico; 3) diffamare qualcuno; 4) utilizzare il nome o l'immagine di una persona per scopi commerciali senza il loro consenso.

sociale ed espressiva, dove assume importanza il modo in cui l'individuo sviluppa la propria personalità attraverso le relazioni nella società.

Mappa concettuale 2 – Evoluzione del Diritto alla Privacy negli USA



L'evoluzione del concetto di privacy in Europa: un percorso giuridico lungo e complesso

Rispetto agli Stati Uniti, l'evoluzione del concetto di privacy in Europa ha seguito un percorso decisamente più articolato. Questo è stato influenzato dalla varietà dei sistemi legali europei e dalle notevoli differenze tra le leggi nazionali degli Stati membri, che hanno reso difficile raggiungere un consenso sulla questione del diritto alla privacy.

Nel 1950, il Consiglio d'Europa[27] ha compiuto un passo significativo per lo sviluppo legale della privacy con l'approvazione della Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU)[28]. Questa convenzione ha introdotto il diritto al rispetto della vita privata e ha istituito la Corte europea dei diritti dell'uomo[29] a Strasburgo. La giurisprudenza di questa corte è stata un fattore chiave nell'affermazione del ruolo centrale della tutela della privacy in Europa.

Negli anni '70, con l'avvento dei primi sistemi automatizzati di gestione delle informazioni, la dottrina e la giurisprudenza nazionali (a cui in alcuni casi è seguito il Legislatore) hanno iniziato a concentrarsi sul trattamento e il controllo dei dati personali. La Germania è stata pioniera con la legge sulla protezione dei dati personali del 1977, seguita dalla Francia nel 1978. La Spagna, nello stesso anno, ha inserito il diritto alla protezione dei dati personali nella sua Costituzione. La giurisprudenza europea ha dunque contribuito a definire il concetto di privacy al di fuori di ciascun Paese membro e già dal 1979, la protezione dei dati

[27] Il Consiglio d'Europa ha l'obiettivo di promuovere la democrazia, i diritti umani e lo Stato di diritto in tutta Europa e altrove. Non va confuso con il Consiglio dell'Unione europea (l'art. 13 del Trattato sull'Unione Europea lo definisce Consiglio, ma è noto anche come Consiglio dei ministri europei, in precedenza come Consiglio speciale dei ministri) che assieme al Parlamento europeo detiene il potere legislativo, né con il Consiglio europeo che ha invece il compito di definire le priorità e gli orientamenti politici generali dell'Ue.

[28] Convenzione europea dei diritti dell'uomo (CEDU) https://eur-lex.europa.eu/IT/legal-content/glossary/european-convention-on-human-rights-echr.html

[29] Corte europea per i diritti dell'uomo (European Court of Human Rights) https://www.echr.coe.int/

personali è stata considerata come parte integrante del diritto alla vita privata della persona.

Si giunge al 1981 e compare la prima iniziativa legislativa a livello europeo per regolamentare l'elaborazione dei dati personali, ovvero la Convenzione n. 108[30] del Consiglio d'Europa, che mira a garantire il diritto alla vita privata in relazione all'automatizzazione del trattamento dei dati personali correlati alla persona stessa. L'obiettivo principale della Convenzione, infatti, è assicurare che in ogni Stato membro partecipante, indipendentemente dalla nazionalità o dalla residenza, ogni individuo goda del rispetto dei suoi diritti e delle sue libertà fondamentali.

Nei seguenti anni ’90 le Istituzioni europee si sono attivamente occupate di affrontare le sfide poste dalle nuove tecnologie e dalla diffusione globale delle reti, espandendo il quadro normativo originariamente delineato dalla prima Direttiva Europea 95/46/CE del 1995[31].

La sopracitata direttiva del 1995 è stata concepita con l'obiettivo di agevolare la libera circolazione dei dati personali tra gli Stati membri, superando le barriere create dalle varie misure di protezione. Inoltre, mirava a garantire la protezione dei diritti fondamentali delle persone fisiche. Questa legislazione, che si rifaceva ai principi stabiliti nella Convenzione del Consiglio d'Europa n. 108 del 1981 in merito alla salvaguardia delle persone nel contesto del trattamento automatizzato dei dati personali, è stata in seguito recepita progressivamente in tutte le legislazioni europee, tra cui l’Italia nel 1996[32].

---

[30] La Convenzione n. 108 del Consiglio d'Europa, o anche Convenzione di Strasburgo del 1981, “Convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati a carattere personale”, rappresenta uno dei più importanti strumenti legali per la protezione delle persone rispetto al trattamento automatizzato dei dati personali. È l'unico strumento giuridicamente vincolante a livello internazionale in tale materia, potendo ad essa aderire anche Stati non membri dell’Unione Europea e del Consiglio d'Europa stesso.

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

[32] Legge n. 675 del 31 dicembre 1996 - Tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali.

In un susseguirsi di sviluppi a partire dalla Direttiva del 1995, la Commissione europea ha intrapreso un'azione costante per adattarsi alle evoluzioni tecnologiche e alla crescente globalizzazione delle reti.

Le corti di giustizia europee hanno progressivamente avviato un processo di armonizzazione delle diverse interpretazioni nazionali, dirigendosi verso un modello unificato. La Corte europea dei diritti dell'uomo sulla base dell'art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali[33], ha sviluppato nel tempo una nozione completa di protezione della vita privata, mentre la Corte di giustizia dell'Unione europea ha delineato il modello europeo di tutela dei dati personali.

Fa seguito, nel 1997, la Direttiva Europea 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni che, in considerazione della prospettiva dell'apertura dei mercati e della crescente evoluzione della tecnologia nel settore delle telecomunicazioni, assicurerà un nuovo e adeguato livello di riservatezza dei dati personali.

Allo scopo di garantire che le istituzioni e gli organi dell'Ue rispettino il diritto dei cittadini al trattamento riservato dei dati personali, spicca l'istituzione del Garante europeo per la protezione dei dati (GEPD)[34].

Dal 2010, la Commissione europea ha avviato un piano di revisione per affrontare le nuove modalità con cui i dati personali vengono raccolti, organizzati ed utilizzati. Questo piano ha portato, all'inizio del 2012, alla presentazione di una proposta di riforma delle normative europee in materia di protezione dei dati.

Questo crescente interesse alla privacy può essere in parte attribuito all'importanza assegnata alla Carta dei diritti fondamentali dell'Unione

[33] CEDU art. 8 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) disciplina il diritto al rispetto della vita privata e familiare, del domicilio e della Corrispondenza.
https://www.giustizia.it/cmsresources/cms/documents/guida_cedu_articolo8_agg31ago2021.pdf

[34] European Data Protection Supervisor (EDPS) https://edps.europa.eu/_en

europea[35]. Questa Carta ha concluso il processo di costituzionalizzazione dell'individuo, un processo precedentemente avviato e inizialmente delineato dalla Legge fondamentale tedesca e dalla Costituzione italiana. Con la nota iniziale che afferma che l'Unione "*pone la persona umana al centro della sua azione*"[36], gli articoli successivi completano un quadro complessivo che definisce come la persona si inserisce nel contesto dei diritti. L'inviolabilità dell'individuo diviene così un mezzo per proteggere la dignità della persona, grazie al controllo dei dati che ne definiscono l'identità digitale. Questo legame tra dignità, informazioni personali, costruzione dell'identità e riconoscimento individuale, crea una connessione indissolubile, evidenziando l'importanza di come i dati personali debbano esser raccolti, organizzati e trattati.

Nel Titolo II della Carta, dedicato alle libertà, viene riconosciuto non solo il diritto fondamentale al "*rispetto della vita privata e familiare*", ma anche il diritto di ciascun individuo alla "*protezione dei dati di carattere personale che lo riguardano*". La Carta stabilisce le modalità e i limiti del trattamento di tali dati, prevedendo anche l'istituzione di un'autorità indipendente per il controllo del rispetto della disciplina in materia. Attraverso questo approccio, la dignità si fonde con i principi di libertà ed uguaglianza, allo scopo di prevenire discriminazioni o stigmatizzazioni sociali.

La Carta presenta quindi una visione moderna della protezione della vita privata, garantendo che l'individuo non perda l'autonomia nella creazione della propria sfera privata e che la sua identità non sia vulnerabile rispetto a decisioni altrui. Si sottolinea così l'importanza dell'identità, che si sviluppa attraverso un processo complesso, fluido e continuamente adattabile alle molteplici relazioni che ciascuno di noi intrattiene nella società e alla loro naturale evoluzione nel tempo.

---

[35] La Carta dei diritti fondamentali dell'Unione europea (la Carta) tutela i diritti fondamentali di cui godono le persone nell'Unione europea (Unione). Strumento moderno e completo del diritto dell'Unione che tutela e promuove i diritti e le libertà delle persone di fronte ai cambiamenti nella società, al progresso sociale e agli sviluppi scientifici e tecnologici.

[36] G. RAMACCIONI, La protezione dei dati personali e il danno non patrimoniale - Jovene Editore, Napoli, 2017, p. 70.

Nel 2016 il Legislatore europeo approva il Regolamento Generale sulla Protezione dei Dati (GDPR), entrato in vigore il 25 maggio 2018, che rappresenta una vera rivoluzione in materia e -di fatto- un punto di svolta significativo in chiave di standardizzazione, nella regolamentazione della privacy e della protezione dei dati personali all'interno dell'Unione europea. Il GDPR è stato introdotto con l'obiettivo di creare un quadro normativo unico e moderno, uniforme e rigoroso, per garantire la privacy dei cittadini dell'Unione europea nell'era digitale. L'intenzione nasce con l'obiettivo di affrontare le sfide poste dalla rapida evoluzione delle tecnologie e dell'elaborazione dei dati personali, nonché di rafforzare i diritti degli individui sulla gestione dei propri dati.

Una delle innovazioni fondamentali del GDPR è stata l'espansione dell'ambito di applicazione: mentre la precedente Direttiva del 1995 si applicava principalmente alle aziende europee, il GDPR si estende a tutte le organizzazioni che trattano dati personali di cittadini europei, indipendentemente dalla loro ubicazione globale. Ciò ha consentito di affrontare con una maggior compiutezza le sfide connesse al trattamento dei dati in un contesto internazionale sempre più complesso. Il GDPR ha portato innovazioni rilevanti nel panorama della tutela dei dati personali, mettendo in evidenza il concetto di accountability.

Centrale è l'accento posto sulla responsabilizzazione delle organizzazioni. Infatti, oltre al "*titolare del trattamento*"[37], il Regolamento introduce due nuovi ruoli, ossia il "*responsabile del trattamento*" (DP - Data Processor)[38] e il

[37] GDPR art. 4, punto 7 "T*itolare del trattamento: 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*."

[38] GDPR art. 4, punto 8 "R*esponsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*." L'organizzazione deve nominare il responsabile della protezione dei dati se le attività principali comportano il trattamento di dati sensibili su vasta scala o comportano un monitoraggio su vasta scala, regolare e sistematico delle persone. A tale riguardo, il monitoraggio del comportamento delle persone interessate comprende tutte le forme di monitoraggio e profilazione su Internet, anche ai fini della pubblicità comportamentale. Le Amministrazioni pubbliche hanno

"*responsabile della protezione dei dati*" (DPO - Data Protection Officer)[39], il che significa che le imprese, le organizzazioni, ecc., sono tenute a designare (in alcuni casi sono obbligate a farlo[40]) persone che si occupino rispettivamente della gestione dei dati (il responsabile del trattamento) e della conformità alle norme (responsabile della protezione dei dati).

Un altro aspetto significativo del GDPR è rappresentato dal principio di "*privacy by design*" in quale afferma che la protezione dei dati deve essere integrata fin dall'inizio, ovvero nativamente, in qualsiasi progetto o applicazione, anziché essere aggiunta successivamente. Ciò promuove una maggiore prevenzione dei rischi e una migliore tutela dei dati.

Inoltre, il Regolamento pone un'enfasi sulla trasparenza e sulla richiesta di consenso (consent) dell'interessato[41] per il trattamento dei dati personali. Le

---

sempre l'obbligo di nominare un responsabile della protezione dei dati (ad eccezione dei tribunali che agiscono nell'esercizio delle loro funzioni giudiziarie).

Il responsabile della protezione dei dati può essere un membro del personale della organizzazione o può essere assunto esternamente sulla base di un contatto di servizio. Il responsabile della protezione dei dati può essere una persona fisica o giuridica.

[39] GDPR art. 4 Sezione 4 "*Responsabile della protezione dei dati*". È la figura che affianca il titolare e/o il responsabile del trattamento per le funzioni di supporto, controllo e prassi formative e informative sulle disposizioni previste dal GDPR.

[40] Le amministrazioni pubbliche hanno sempre l'obbligo di nominare un responsabile della protezione dei dati (ad eccezione dei tribunali che agiscono nell'esercizio delle loro funzioni giudiziarie). La designazione del responsabile della protezione dei dati è obbligatoria, ad esempio, quando la azienda/organizzazione è: 1) un ospedale che tratta grandi serie di dati sensibili; 2) una società di sicurezza incaricata di monitorare i centri commerciali e gli spazi pubblici; 3) una piccola società di head-hunting che profila le persone. Il responsabile della protezione dei dati non è obbligatorio se: 1) si è un medico di una comunità locale e tratti i dati personali dei pazienti; 2) si ha un piccolo studio legale e si trattano i dati personali dei propri clienti. La designazione del DPO è obbligatoria in tre ipotesi: 1) se il trattamento di dati personali è effettuato da un'autorità pubblica o da un organismo pubblico; 2) quando le attività principali dell'organizzazione consistono in trattamenti che, richiedono il "*monitoraggio regolare e sistematico*" degli interessati "*su larga scala*"; 3) quando le attività principali dell'organizzazione consistono nel trattamento "su larga scala" di dati "*sensibili*" (rectius, "*categorie particolari di dati*") o "*giudiziari*" (rectius, "*dati personali relativi a condanne penali e reati*").

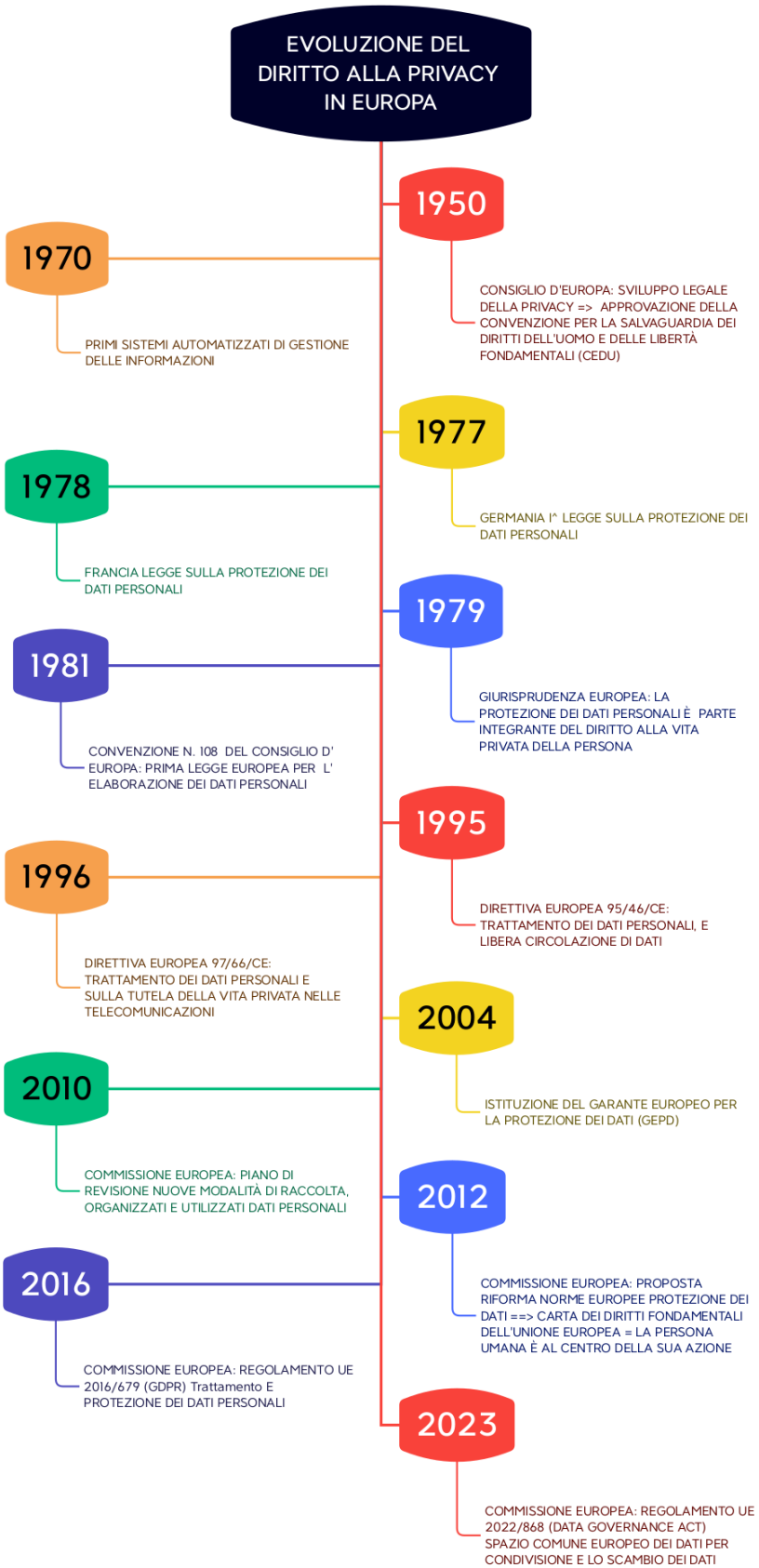
[41] GDPR art. 4, punto 11 "*consenso dell'interessato: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento."*

organizzazioni sono tenute a spiegare in modo chiaro e comprensibile come verranno utilizzati i dati e a ottenere un consenso chiaro e volontario dagli interessati.

Il GDPR rafforza anche i diritti degli individui sui propri dati personali. Gli interessati hanno il diritto di accedere ai propri dati, di richiederne la correzione o la cancellazione e di ottenere la portabilità dei dati. Questi diritti conferiscono maggiore controllo alle persone sulla gestione delle proprie informazioni personali.

Infine, il GDPR introduce un regime sanzionatorio più severo per le organizzazioni che non rispettano le disposizioni del Regolamento e questo ha spinto le aziende a investire maggiormente nella sicurezza delle informazioni e a prendere sul serio la protezione dei dati.

Mappa concettuale 3 – Evoluzione del diritto alla Privacy in Europa



Il diritto alla riservatezza in Italia

In Italia, l'interesse verso la questione della riservatezza ha radici che risalgono agli anni '50 del secolo scorso, quando l'argomento della privacy cominciò a essere inquadrato all'interno del più ampio contesto dei diritti individuali. In modo diverso da alcuni altri paesi europei e, soprattutto, dagli Stati Uniti d'America, in Italia, la necessità di normative in questo campo si rese evidente con una maggiore inerzia.

La mancanza di una norma chiara sul diritto alla privacy ha portato a diverse teorie nel dibattito dottrinale. Alcune teorie sono a sostegno dell'esistenza di un diritto autonomo alla riservatezza, mentre altre lo negano come una situazione giuridica. All'interno di questo dibattito, il ruolo della giurisprudenza, a partire dalla metà del '900, è stato di vitale importanza.

La nozione di riservatezza nell'evoluzione della giurisprudenza della Corte di cassazione ha seguito un percorso significativo, e un momento cruciale è rappresentato dalla sentenza n. 4487/1956[42], noto come il "caso Caruso". In questa sentenza, la Corte di cassazione affrontò la questione dell'esistenza di un diritto alla riservatezza. Il caso riguardava due film sulla vita del celebre tenore Enrico Caruso. Questi film includevano episodi romanzati della sua vita privata, considerati dalla sua famiglia come lesivi della sua riservatezza artistica e personale. La Corte di cassazione, in questa fase iniziale, negò l'esistenza di un diritto alla riservatezza in questa situazione specifica. Questa decisione è stata fondamentale per tracciare il confine tra la sfera pubblica e privata di una figura pubblica come Caruso. La Cassazione stabilì che, nonostante le rappresentazioni romanzate della sua vita privata nei film, non si poteva affermare che tali episodi violassero un diritto di riservatezza. Questa sentenza ha indicato una visione

[42] Cass. Civ. 22 dicembre 1956, n. 4487; secondo cui: "*Nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto, non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto.*" https://www.jstor.org/stable/23146612

iniziale che tendeva a limitare l'ambito del diritto alla riservatezza, in particolare quando coinvolgeva personaggi pubblici o figure notorie.

Successivamente, la sentenza n. 990/1963[43], nota come il "caso Petacci", rappresenta un momento chiave nel mutamento di prospettiva riguardo alla nozione di riservatezza all'interno della giurisprudenza italiana. Questa sentenza ha affrontato il tema dell'equilibrio tra il diritto alla riservatezza, da un lato, e la libertà di espressione, dall'altro. Il caso riguardava la pubblicazione di una biografia in cui si narrava la relazione di Claretta Petacci e Benito Mussolini, ritenuta lesiva della riservatezza e della reputazione dei soggetti coinvolti. La Corte di cassazione, con questa decisione, ha iniziato a spostare l'accento dalla mera negazione del diritto alla riservatezza verso un approccio più bilanciato tra i diritti fondamentali coinvolti. In particolare, la Corte ha riconosciuto che il diritto alla riservatezza può entrare in conflitto con la libertà di espressione e il diritto di informazione. Tuttavia, ha chiarito che l'esercizio di questi diritti non dovrebbe ledere in modo ingiustificato la dignità, la reputazione e la sfera privata delle persone coinvolte.

La sentenza del "caso Petacci" ha aperto la strada a una prospettiva più articolata sulla riservatezza, sottolineando la necessità di considerare attentamente il bilanciamento tra i diritti costituzionali in gioco. Questo cambiamento di approccio ha gettato le basi per ulteriori sviluppi nella giurisprudenza successiva, in cui il diritto alla riservatezza è stato sempre più riconosciuto e bilanciato rispetto ad altri interessi fondamentali

Nel 1975, la sentenza n. 2129/1975[44], conosciuta come il "caso Soraya", rappresenta un punto di svolta nella giurisprudenza italiana riguardo al diritto

[43] Cass. civ. 20 aprile 1963, n. 990 (cd. caso Petacci), in Foro it, secondo cui: "S*ebbene non sia ammissibile il diritto tipico alla riservatezza, viola il diritto assoluto di personalità, inteso quale diritto erga omnes alla libertà di autodeterminazione nello svolgimento della personalità dell'uomo come singolo, la divulgazione di notizie relative alla vita privata, in assenza di un consenso almeno implicito, ed ove non sussista, per la natura dell'attività svolta dalla persona e del fatto divulgato, un preminente interesse pubblico di conoscenza.*"

[44] Cass. civ., Sez. I, 27 maggio 1975, n. 2129 (cd. caso Soraya), in Foro It, secondo cui: "*Il nostro ordinamento riconosce il diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori del domicilio domestico,*

alla riservatezza. In questo caso, la Corte di cassazione ha affrontato il tema della pubblicazione di foto che ritraevano l'ex imperatrice Soraya Esfandiary in momenti intimi all'interno della sua abitazione. Questa sentenza ha segnato il riconoscimento esplicito e il consolidamento del diritto alla riservatezza nell'ambito giuridico italiano. L'evoluzione della giurisprudenza di merito, nel frattempo, aveva creato un solido fondamento per questo riconoscimento. La Corte ha affermato che il diritto alla riservatezza è parte integrante del complesso dei diritti della personalità e che la sua tutela è fondamentale per preservare la dignità e la sfera privata degli individui. Nel caso specifico, la Corte ha considerato che la pubblicazione delle foto riprese all'interno della casa di Soraya Esfandiary, in momenti considerati intimi, costituiva una violazione della sua riservatezza e della sua dignità. Questa sentenza ha contribuito a consolidare la nozione di riservatezza come un diritto soggettivo autonomo e ha stabilito criteri chiari per valutare le situazioni in cui il diritto alla riservatezza potrebbe entrare in conflitto con altri interessi, come la libertà di espressione. La decisione ha anche aperto la strada a una serie di sviluppi successivi nella giurisprudenza italiana, contribuendo a delineare ulteriormente i confini e le caratteristiche del diritto alla riservatezza nel contesto dell'evoluzione tecnologica e della diffusione globale delle informazioni

Più di recente, la sentenza n. 1652/1994[45] rappresenta un importante passo avanti nella giurisprudenza italiana in materia di privacy, introducendo il concetto del "diritto ad essere lasciati soli" (right to be left alone). Questa sentenza ha ulteriormente contribuito a consolidare e ampliare la nozione di riservatezza e di protezione della sfera personale degli individui. Nel caso affrontato dalla sentenza, venne contestata la registrazione audio effettuata senza consenso di una conversazione privata tra due persone. La Corte di cassazione sottolineò che il diritto alla riservatezza non si limitava solo a

non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti."

[45] Cass. 21 febbraio 1994, n. 1652, in Giur. it., 1995

prevenire la divulgazione non autorizzata di informazioni personali, ma si estendeva anche a garantire il diritto delle persone ad essere lasciate sole e a mantenere la loro privacy in ambienti confidenziali. La sentenza ha contribuito a sottolineare l'importanza di proteggere non solo l'aspetto informativo della riservatezza, ma anche l'ambiente in cui si svolgono le conversazioni e le comunicazioni private. Ha stabilito che la violazione di questo "diritto ad essere lasciati soli" costituiva una lesione del diritto alla riservatezza e, di conseguenza, poteva essere soggetta a sanzioni. La sentenza n. 1652/1994 ha dunque aggiunto un nuovo elemento alla comprensione del diritto alla riservatezza, riconoscendo che la protezione della privacy non riguarda solo l'informazione personale, ma anche la creazione di spazi confidenziali in cui le persone possano sentirsi al sicuro da intrusioni indesiderate. Questa sentenza ha contribuito a rafforzare ulteriormente la protezione dei diritti della personalità e la sfera privata degli individui nell'ambito giuridico italiano. Si può dunque affermare che "*la Cassazione oggi riconosce pienamente l'esistenza di una giurisprudenza e dottrina consolidate in ordine all'esistenza, nel nostro ordinamento, di un diritto alla riservatezza*."[46]

Dal punto di vista legislativo, invece, l'Italia ha introdotto più di recente varie specifiche normative sulla protezione dei dati personali, inizialmente con la legge n. 675 del 31 dicembre 1996 e successivamente con il Decreto Legislativo 196/2003, noto come Codice sulla protezione dei dati personali. Da ultimo con il Decreto Legislativo n. 101/2018 il Legislatore nazionale è intervenuto al fine di armonizzare la suddetta norma nazionale del 2003 con quelle introdotte successivamente dal Legislatore europeo (il GDPR).

Oggi, dunque, ci troviamo di fronte ad un impianto normativo in materia di protezione dei dati personali che opera su due livelli distinti.

- In primo luogo, troviamo una norma di fonte di diritto derivato europeo, il Regolamento Generale sulla Protezione dei Dati (GDPR), che si applica dal

[46] Prosperi M. Il dibattito italiano sull'esistenza e sul fondamento del diritto alla riservatezza prima del suo espresso riconoscimento, https://www.privacy.it/archivio/prosperi200206.html

25 maggio 2018. Il Regolamento che, come già accennato, è atto tipico e possiede le qualità della generalità, della obbligatorietà e -soprattutto- la diretta applicabilità, è vincolante per tutti gli Stati Membri dell'Unione europea e stabilisce obblighi e requisiti uniformi che devono essere rispettati da ciascun paese membro.

- In secondo luogo, vi è il quadro normativo nazionale, rappresentato dal Codice per la protezione dei dati personali (Decreto Legislativo 196/2003), che ha regolamentato la privacy fin dal 2003. Inoltre, il già menzionato Decreto Legislativo n. 101/2018 ha aggiunto ulteriori disposizioni e adeguamenti alla normativa italiana in conformità con il GDPR.

Questo sistema a doppio livello fornisce una base normativa sia a livello europeo che nazionale, garantendo un quadro coerente e solido per la protezione dei dati personali e la privacy.

Dalla privacy alla protezione dei dati personali

I concetti di privacy e protezione dei dati personali rappresentano un aspetto chiave dell'evoluzione normativa, con implicazioni profonde e significative. Mentre ad un occhio superficiale la distinzione tra privacy e protezione dei dati potrebbe apparire sfuggente, si tratta in realtà di diritti ben distinti, che rispondono a interessi differenti e che hanno avuto una distinta origine.

La privacy, intesa come tutela della sfera privata, si concentra sulla protezione da intrusioni indesiderate da parte di privati, aziende o altre persone. Diverse sono invece le preoccupazioni legate all’ingerenza dello Stato.

L'introduzione dell'articolo 8 della Convenzione europea dei Diritti dell'Uomo (CEDU) nel 1950 sancisce il diritto al rispetto della vita privata, concentrandosi sulla protezione della sfera individuale dall'ingerenza statale. Questo concetto è ulteriormente sancito dall'articolo 2 della Costituzione italiana del 1947, che riconosce e garantisce i diritti inviolabili dell'individuo.

Nel 1978, in risposta al contesto politico dell'epoca, la Germania Federale introduce la prima legge nazionale per la protezione dei dati personali. Questa

mossa nasce come reazione al pericolo ed alla paura della dittatura, per ovvi motivi storici, riconoscendo il potenziale per il potere statale di rafforzarsi attraverso il trattamento dei dati personali.

Nel 1981, come già affrontato, il Consiglio d'Europa adotta la Convenzione 108 sulla protezione dei dati personali, che diventa un importante riferimento in Europa. La definizione di dati personali come informazioni relative a individui identificati o identificabili viene introdotta, insieme all'importanza di proteggere la libertà individuale da controlli esterni.

Con la diffusione dei personal computer e di Internet, negli anni '90 sono emerse nuove sfide per la privacy che hanno coinvolto principalmente le autorità governative, ma hanno anche iniziato ad affacciarsi preoccupazioni legate alle aziende e alla tecnologia stessa. Con la crescente adozione dei computer e la navigazione in rete, i fornitori di servizi Internet (Internet Service Provider - ISP) e le aziende online hanno iniziato a raccogliere dati sugli utenti, come indirizzi IP, cronologia di navigazione e abitudini di utilizzo, ecc. Questi dati sono stati inizialmente utilizzati per scopi di marketing e per migliorare l'esperienza dell'utente, ma hanno sollevato preoccupazioni sulla privacy in quanto rivelavano informazioni personali. Sono stati introdotti i "cookies"[47] per raccogliere informazioni sul comportamento di navigazione. Sebbene fossero spesso utilizzati per scopi legittimi, come il mantenimento delle sessioni utente, sono diventati strumenti per il tracciamento degli utenti online, sollevando domande sulla privacy e sulla gestione dei dati personali. Inoltre, l'uso diffuso della posta elettronica e delle comunicazioni online ha sollevato domande sulla sicurezza e sulla privacy delle comunicazioni digitali. L'accesso non autorizzato alle e-mail e la possibilità di intercettare le comunicazioni hanno suscitato crescenti preoccupazioni riguardo alla privacy. Con l'ampia diffusione di Internet tra i giovani, è sorta la preoccupazione per la loro sicurezza online. Inoltre, a mano

[47] In informatica, file di servizio che viene inviato da un sito Internet all'utente che si collega con esso, allo scopo di registrarne l'accesso e di lasciare sullo schermo un'icona che renda immediato il collegamento in una successiva circostanza. Talvolta con il termine c. si indica anche l'icona stessa, enciclopedia on line Treccani https://www.treccani.it/enciclopedia/cookie/

a mano che le transazioni online sono diventate sempre più comuni, si è manifestata una crescente preoccupazione per la sicurezza dei dati personali nelle transazioni economiche e per i trasferimenti di denaro, come ad esempio i numeri delle carte di credito. Per affrontare tali questioni, sono state sviluppate tecnologie di crittografia per proteggere le transazioni online, anche se ciò ha sollevato interrogativi riguardo alla possibilità di accessi non autorizzati e alle potenziali violazioni della sicurezza.

Sebbene in quel periodo la privacy fosse in gran parte associata alle attività online, con l'evolversi della tecnologia, queste preoccupazioni si sono ampliate includendo anche questioni relative alle aziende e all'utilizzo dei dati personali.

Con il passaggio all'Unione europea ed al mercato unico europeo nel 1993[48], il problema della standardizzazione delle norme sulla protezione dei dati diventa rilevante. La Direttiva 95/46/CE viene adottata dalla allora Comunità europea per affrontare questa sfida, stabilendo regole per il trattamento dei dati personali all'interno dell'UE.

In un susseguirsi di sviluppi a partire dalla Direttiva del 1995, la Commissione europea ha, come si è visto, intrapreso un'azione costante per adattarsi alle evoluzioni tecnologiche e alla crescente globalizzazione delle reti. Fin dal 2010, la Commissione europea ha avviato un piano di revisione per affrontare le nuove modalità con cui i dati personali vengono raccolti, organizzati ed utilizzati. Questo piano ha portato, all'inizio del 2012, alla presentazione di una proposta di riforma globale delle normative europee in materia di protezione dei dati.

Questo crescente interesse alla sfera della privacy può essere in parte attribuito all'importanza assegnata alla Carta dei diritti fondamentali dell'Unione europea. Questa Carta ha concluso il processo di costituzionalizzazione dell'individuo, un processo precedentemente avviato e chiaramente delineato da alcune

[48] Il mercato unico è tra i più importanti successi dell'integrazione europea e uno dei suoi motori principali. Istituito il 1° gennaio 1993, il mercato unico europeo consente a merci, servizi, persone e capitali di circolare liberamente nell'UE, semplificando la vita delle persone e aprendo nuove opportunità alle imprese.
https://www.politicheeuropee.gov.it/it/comunicazione/approfondimenti/30-anni-di-mercato-unico/

Costituzioni nazionali. Con il Preambolo che afferma che l'Unione "*pone la persona umana al centro della sua azione*", gli articoli successivi completano un quadro complessivo che definisce come la persona si inserisce nel contesto dei diritti.

Fondamentale è il rispetto per la dignità umana, che costituisce il principio guida entro il quale si sviluppano le relazioni personali. La Carta attribuisce un ruolo cruciale alla tutela dell'individuo, riconoscendogli il pieno controllo delle decisioni legate all'innovazione scientifica e tecnologica e sottolineando il suo potere di supervisione sulla sfera personale, inclusa la sua "*identità elettronica*", rappresentata dai dati personali nella rete. Questi dati giocano un ruolo fondamentale nella formazione dell'identità individuale e della reputazione di ciascuno.

In Italia la legge n. 675 del 31 dicembre 1996 non ha semplicemente attuato la normativa europea, ma ha anche introdotto un aspetto cruciale per l'evoluzione delle norme. Oltre alla tutela dei diritti e delle libertà fondamentali, ha sottolineato la necessità che il trattamento dei dati personali rispettasse la dignità individuale, estendendo la protezione all'identità personale. Tale norma ha svolto un ruolo rilevante, disciplinando due figure giuridiche precedentemente definite dalla giurisprudenza: il diritto alla riservatezza e il diritto all'identità personale.

Oltre alle innovazioni rispetto alla normativa europea, la legislazione italiana ha individuato alcune forme di persecuzione che possono derivare dal trattamento dei dati personali, come ad esempio la perdita della propria serenità individuale in conseguenza di un'utilizzazione dei dati che riguardano la propria intimità oppure la distorta rappresentazione della propria identità sociale, tale da arrecare pregiudizio alle interazioni quotidiane. Le moderne tecnologie e le nuove modalità di circolazione delle informazioni possono mettere a rischio il diritto alla protezione dei dati personali. Questi rischi includono la perdita di tranquillità a causa dell'abuso dei dati, la distorsione dell'identità sociale che compromette le relazioni quotidiane e la perdita dell'autonomia decisionale a causa dell'informazione indiscriminata che influisce sulla sfera giuridica.

La legislazione italiana mira a proteggere non solo i dati in sé, ma attraverso questa protezione, tutela l'unicità dell'individuo. Questa prima legge di protezione della privacy ha superato la concezione tradizionale di questo diritto, aprendo la strada all'accesso alle informazioni relative alla persona per controllarne l'accuratezza, correggere gli errori e monitorarne l'uso nel tempo. In definitiva, la privacy si è rivelata un diritto multifunzionale, in grado di affrontare molteplici sfaccettature e offrire una tutela olistica alla persona, la cui identità è sempre più intrecciata con i dati che la riguardano.

La Corte di cassazione ha compiuto un'analisi approfondita della nozione di diritto alla riservatezza, anche dopo l'entrata in vigore della legge n. 675 del 1996. Con la sentenza n. 5658 del 9 giugno 1998[49], la Corte ha riconosciuto ormai l'esistenza di un vero e proprio diritto alla riservatezza, al di là delle situazioni espressamente previste dalla legge, integrandolo nel sistema di protezione costituzionale della persona.

Tuttavia, con il proliferare dell'informatica di massa, si rende necessario un quadro normativo più robusto. Approvato dal Legislatore europeo nel 2016, il Regolamento Generale sulla Protezione dei Dati (GDPR) entra in vigore nel 2018, sostituendo la Direttiva precedente.

Inoltre, il GDPR sottolinea l'importanza dell'accountability, spostando l'attenzione dalla semplice adesione alle norme al dimostrare concretamente le misure intraprese per proteggere i dati personali. Questo concetto richiede alle organizzazioni di essere responsabili e trasparenti nella gestione dei dati, dimostrando il loro impegno per la tutela della privacy degli individui.

Oggi, dunque, per DATO PERSONALE si intende:

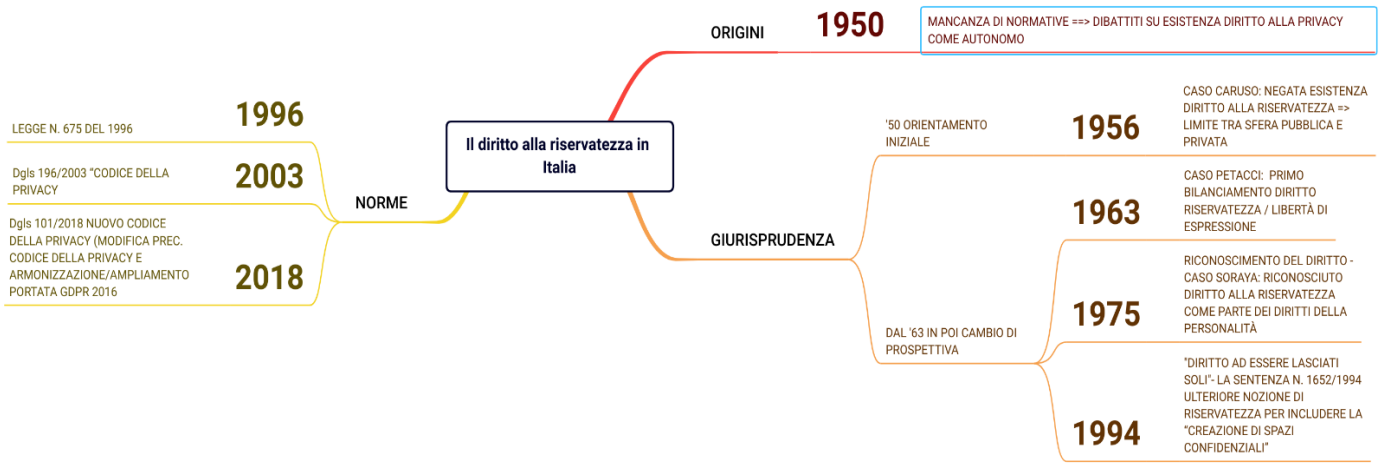
> "*qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare*

[49] Cass. civ. 9 giugno 1998 n. 5658, Roma (L'utilità sociale dell'informazione su un fatto di cronaca può non essere sufficiente a giustificare la pubblicazione dei nomi dei suoi protagonisti) https://www.studiozallone.it/wp-content/uploads/2019/12/Cass.-9.6.98-5658-Diritto-di-cronaca-e-riservatezza-bilanciamento-di-diritti-2.pdf

riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale."[50]

[50] GDPR art. 4 - Definizioni, punto 1

Mappa concettuale 4 - Il diritto alla riservatezza in Italia



L'era dell'Information and Communication Technologies (ICT)

Nell'era della società digitale, l'ascesa di nuovi strumenti di comunicazione e diffusione delle informazioni ha permesso l'accumulo e la condivisione praticamente illimitata di dati. Questa situazione rappresenta una sfida cruciale per garantire la tutela adeguata dei dati personali. Le tecnologie in continua evoluzione si basano sulla costante circolazione dei dati e queste innovazioni hanno un impatto diretto sulla questione della privacy.

Nel quadro del dibattito sulla privacy, è evidente che i recenti progressi tecnologici hanno sollevato profonde preoccupazioni tra coloro che difendono la riservatezza. L'ampliamento dei sistemi di telecomunicazione connessi agli ormai comuni dispositivi (devices*)* quotidiani, ha rappresentato un passo significativo verso una realtà in cui l'interazione online rivelerà sempre più aspetti della nostra vita. Si pensi ad esempio, all'uso diffuso dei social media o alla proliferazione di tecnologie come i big data (dati raccolti, ad esempio, da smartphone o smartTV, da transazioni con carte di credito, da sensori di videosorveglianza connessi ai servizi di trasporto urbano, ecc.)[51], il cloud computing (come, ad esempio, Gmail, Google Drive, Google Calendar, ecc.)[52] e il già menzionato IoT, che hanno reso l'accesso alle informazioni una risorsa inesauribile. Le informazioni così

[51] "*La Commissione europea prevede che il numero totale dei dati crescerà del 530% entro il 2025 rispetto al 2018…"*
https://www.europarl.europa.eu/news/it/headlines/society/20210211STO97614/big-data-definizione-benefici-e-sfide-infografica

[52] Letteralmente "*nuvola informatica*", termine con cui ci si riferisce alla tecnologia che permette di elaborare e archiviare dati in rete. In altre parole, attraverso internet il c.c. consente l'accesso ad applicazioni e dati memorizzati su un hardware remoto invece che sulla workstation locale. Per le aziende di grosse dimensioni implica dunque un ingente abbattimento dei costi; non sono più necessari hardware potenti (costosi e soggetti a frequenti manutenzioni), ma basta una macchina in grado di far funzionare l'applicativo d'accesso alla "*nuvola*". Non mancano però le perplessità; da un lato i file sono accessibili solo tramite rete, dall'altro (nonostante le rassicurazioni dei fornitori) si teme per la sicurezza dei dati sensibili. Il c.c. può mettere a disposizione hardware in remoto (IaaS - Infrastructure as a Service), piattaforme software (PaaS - Platform as a Service) o software in remoto (SaaS - Software as a Service). Enciclopedia online Treccani.
https://www.treccani.it/enciclopedia/cloud-computing

raccolte, grazie alla capacità di memorizzazione e interconnessione dei nuovi apparati, possono potenzialmente e pericolosamente rimanere accessibili per sempre. Pertanto, sebbene le nozioni e i problemi legati alla privacy in generale possano non adattarsi agevolmente al contesto di Internet, è cruciale riconoscere che si tratta comunque di protezione della riservatezza. In questa prospettiva, l'analisi dell'evoluzione giuridica del diritto alla privacy risulta essenziale per adattare le norme generali alle nuove sfide poste dall'uso di Internet.

Una prima complessità consiste nel definire Internet, specialmente nell'ambito giuridico. Nel 1999, ad esempio, l'ordinamento statunitense ne ha fornito una definizione nel Children's Online Privacy Protection Act[53], un atto per la protezione dei dati sensibili dei minori. In questa legge, Internet viene descritto come una rete interconnessa globalmente, composta da computer, servizi di telecomunicazione, software operativi e apparecchiature, che utilizzano il protocollo TCP/IP (Transmission Control Protocol/Internet Protocol)[54] per trasmettere informazioni di ogni tipo. Tuttavia, oltre alle definizioni tecniche, è ormai chiaro a tutti che Internet è uno strumento di comunicazione versatile, veloce e potente, ma non sempre affidabile in termini di riservatezza, sicurezza e veridicità. Questa constatazione sottolinea il ruolo fondamentale della protezione della privacy su Internet, che va oltre il tradizionale concetto di essere lasciati soli. Le attività svolte online da un utente medio sono così varie e delicate da poter mettere a rischio valori come libertà, dignità, sicurezza e benessere individuale.

Su Internet, si ripropone la dialettica tra visibile e invisibile, tra chi osserva e chi è osservato, tra il cercatore e la preda. Le parole stesse rivelano questa realtà: lasciamo tracce digitali che possono essere costantemente seguite e memorizzate. In questo contesto, è importante ricordare che Internet è uno

[53] The Children's Online Privacy Protection Act, Federal Trade Commission. https://www.ftc.gov/business-guidance/privacy-security/childrens-privacy

[54] TCP/IP Lessico del XXI Secolo, Treccani https://www.treccani.it/enciclopedia/tcp-ip_%28Lessico-del-XXI-Secolo%29/

strumento che favorisce opportunità democratiche solo quando è garantito l'anonimato per coloro che si esprimono. Questa invisibilità, tipica delle elezioni, diventa essenziale per esercitare la libertà di espressione e il diritto alla partecipazione politica. Giusto per citare alcuni esempi, i rifugiati politici che desiderano denunciare violazioni dei diritti civili nel loro paese d'origine attraverso Internet, hanno bisogno di preservare l'anonimato per evitare ritorsioni. La stessa considerazione vale per coloro che desiderano finanziare partiti politici: le transazioni finanziarie digitali sono registrate, ma è fondamentale che l'individuo possa sostenere le proprie idee senza timore di ritorsioni o coercizioni. Questo problema è particolarmente rilevante nei paesi sotto regimi totalitari, come documentato dal Rapporto 2004 di Reporters sans frontiéres intitolato "*Internet sous surveillance*"[55], che denuncia la stretta sorveglianza imposta da alcuni stati sulle comunicazioni via modem, inclusa la censura di siti indesiderati e la profilazione degli utenti, spesso senza alcuna garanzia di libertà.

Spostandoci verso la giurisprudenza, la Corte di giustizia europea ha emesso sentenze di grande importanza riguardo alla tutela dei dati personali online. Queste pronunce hanno gettato le basi per riforme legislative negli ultimi anni, riconoscendo il ruolo fondamentale della protezione della privacy rispetto ad altri diritti di libertà individuali.

Una di queste sentenze, ad esempio, riguarda la causa tra Digital Right Ireland Ltd e l'Irlanda nel 2014[56], dove è stata dichiarata l'invalidità della Direttiva 2006/24/CE sulla conservazione dei dati di traffico telefonico e telematico. La Corte ha rilevato che la conservazione di questi dati rappresenta un'ingerenza nei diritti fondamentali delle persone coinvolte e ha concluso che la Direttiva violava il principio di proporzionalità.

[55] Surace M., Evoluzione storico-giuridica del diritto alla riservatezza: da diritto borghese a sinonimo di libertà, 2005 http://www.adir.unifi.it/rivista/2005/surace/cap2.htm#n97

[56] Sentenza della Corte (Grande Sezione) dell'8 aprile 2014, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0293

Un altro importante caso riguarda la sentenza del 2014 nella causa Google Spain contro AEPD[57], in cui è stato riconosciuto il "*diritto all'oblio*". Questo principio sancisce che chiunque può richiedere la rimozione di informazioni personali dai risultati di ricerca online quando tali informazioni non sono più rilevanti o sono inadeguate.

Un ulteriore rilevante sviluppo è stato il caso Schrems II del 2015[58], che ha portato a una ridefinizione degli accordi sulla privacy tra l'Unione europea e gli Stati Uniti[59]. In questo contesto, il trasferimento dei dati personali di cittadini europei verso gli USA è stato messo in discussione, evidenziando conflitti tra esigenze di sicurezza nazionale e diritti individuali. Questa sentenza ha influenzato i rapporti tra le due parti e ha portato alla sostituzione dell'accordo Safe Harbor[60] con il nuovo Privacy Shield[61], che impone obblighi più rigorosi sulla protezione dei dati personali e misure di sicurezza contro l'accesso da parte del governo statunitense.

---

[57] Sentenza della Corte (Grande Sezione) del 13 maggio 2014, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX%3A62012CJ0131

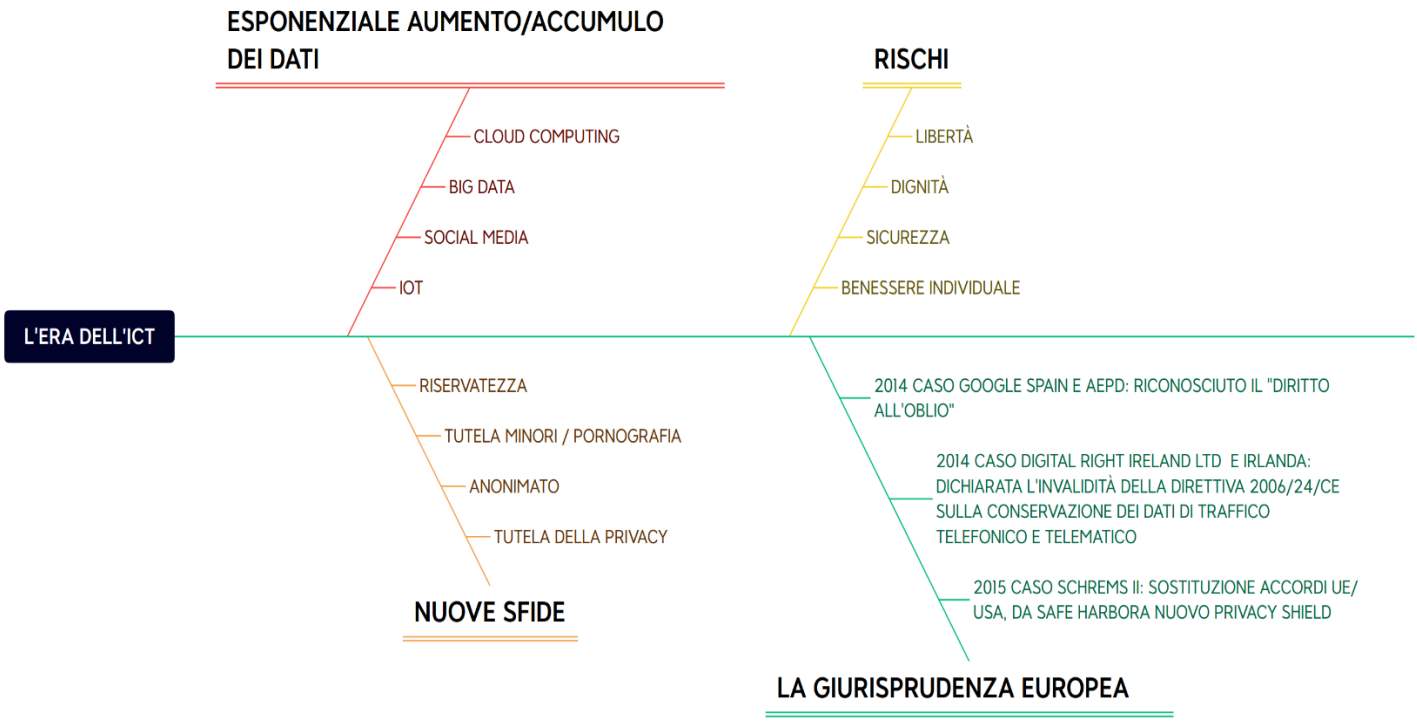
[58] Corte di giustizia dell'Unione europea - COMUNICATO STAMPA n. 91/20 Lussemburgo, 16 luglio 2020, "*La Corte dichiara invalida la decisione 2016/1250 della Commissione sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la privacy*"
https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091it.pdf

[59] Il nuovo accordo fa seguito alle indicazioni della Corte di giustizia europea, che il 6 ottobre 2015 aveva dichiarato non valida la decisione della Commissione del 2000 sullo scambio di dati tra UE e USA, il cosiddetto Safe Harbour
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5306161

[60] Safe Harbour, autorizzazione al trasferimento verso gli Stati Uniti d'America del 10 ottobre 2001
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/30939

[61] Privacy shield, La Commissione europea ha adottato il 12 luglio 2016 una Decisione in merito al cosiddetto Privacy Shield, il nuovo accordo che regolamenta il trasferimento di dati tra Unione europea e USA. La nuova disciplina prevede quanto segue: 1) obblighi di protezione stringenti per le imprese che trasferiscono dati; 2) misure di sicurezza in materia di accesso ai dati da parte del Governo degli Stati Uniti; 3) strumenti specifici per la tutela delle persone; 4) la revisione annuale congiunta dell'accordo per monitorarne l'attuazione
https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/5306161

Mappa concettuale 5 – L’era dell’ICT



L’equilibrio fra diritti fondamentali e libera circolazione delle informazioni

Nella Costituzione Italiana, agli articoli da 1 a 12[62] e nella prima parte relativa ai "*Diritti e doveri dei cittadini*", sono delineati i “*principi fondamentali*”, che costituiscono la base su cui si fonda l'ordinamento costituzionale del nostro Paese. Questo ordinamento subirebbe una trasformazione radicale se tali principi non fossero rispettati e protetti. I valori enunciati, infatti, acquisiscono un'importanza giuridica così significativa da influenzare profondamente l'organizzazione del potere pubblico, orientandola a promuovere ed attuare i principi che tutelano la “*persona*”. Ciò avviene attraverso la tutela dei “*diritti della personalità*”[63]: diritti assoluti, irrinunciabili, inalienabili, intrasmissibili, imprescrittibili, quali ad esempio il diritto alla vita e all’integrità fisica, il diritto all'onore, il diritto alla riservatezza, il diritto all'immagine, il diritto all'identità personale. Nella nostra Costituzione, il fulcro è dunque rappresentato dalla persona, con la sua identità unica e irrinunciabile, su cui si concentrano diritti e doveri. Nell’accezione comune, termini come "*diritti umani*", "*diritti inviolabili*", "*diritti costituzionali*" e "*diritti fondamentali*" sono spesso usati in modo intercambiabile per indicare diritti che dovrebbero essere garantiti a ogni individuo in quanto tale. Questo riflette il legame profondo e intrinseco tra diritto naturale e diritto positivo, un concetto radicato nella comprensione comune.
Dal punto di vista della giurisprudenza, merita attenzione la sentenza della Corte costituzionale n. 13 del 1994[64] poiché essa sottolinea il diritto all'identità

[62] Costituzione della Repubblica Italiana, Principi fondamentali art. 1 - art. 12, Governo Italiano Presidenza del Consiglio dei Ministri https://www.governo.it/it/costituzione-italiana/principi-fondamentali/2839

[63] Oggetto di tutela sia dal punto costituzionale, sia in convenzioni internazionali come la dichiarazione universale dei diritti dell'uomo, adottata dalle Nazioni Unite nel 1948 e la dichiarazione del consiglio d'Europa.

[64] Corte Costituzionale, sentenza n. 13 del 3 febbraio 1994 secondo cui: "*La Corte Costituzionale dichiara l'illegittimità costituzionale dell'art. 165 del Regio decreto 9 luglio 1939, n. 1238 (Ordinamento dello stato civile), nella parte in cui non prevede che, quando la rettifica degli atti dello stato civile, intervenuta per ragioni indipendenti dal soggetto cui si riferisce, comporti il cambiamento del cognome, il soggetto stesso possa ottenere dal giudice il riconoscimento del diritto*

personale come parte essenziale dei diritti umani. Questo diritto implica la libertà di essere sé stessi, con le proprie convinzioni ideologiche, religiose, morali e sociali, che caratterizzano l'individuo. L'identità personale è un valore intrinseco, indipendente dalla situazione sociale ed economica, e la dignità umana, come pilastro del patto costituzionale, si traduce immediatamente nel "*principio personalista*"[65] finalizzato alla sua preservazione.

Il riconoscimento dei diritti fondamentali nella Costituzione rappresenta uno degli elementi distintivi dello Stato di diritto. Questi diritti sono garantiti attraverso la "rigidità" della Costituzione e il controllo esercitato dalla Corte costituzionale; è palese che i diritti fondamentali non soltanto rappresentano il fondamento supremo dell'ordinamento costituzionale, ma contribuiscono anche a modellare la struttura stessa dello Stato democratico.

Qualsiasi limitazione, diminuzione o violazione di questi diritti metterebbe in pericolo la struttura democratica dello Stato.

Ed ancora, la giurisprudenza costituzionale con la sentenza n. 170 del 1984[66], stabilisce che alcuni principi supremi nella Costituzione italiana non possono essere modificati o sovvertiti neppure da leggi di revisione costituzionale o altre leggi costituzionali. Questi principi sono intrinsecamente legati ai valori fondamentali su cui si basa la Costituzione italiana e hanno una priorità superiore rispetto alle altre norme gerarchicamente sotto ordinate ad essa. Inoltre, la

---

a mantenere il cognome originariamente attribuitogli ove questo sia ormai da ritenersi autonomo segno distintivo della sua identità personale."
https://www.gazzettaufficiale.it/atto/corte_costituzionale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1994-02-09&atto.codiceRedazionale=094C0091

[65] La Repubblica Italiana riconosce i diritti inviolabili della persona ed essa è posta al centro, come fissato dall'articolo 2 della Costituzione italiana "*La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica, sociale*"

[66] Corte costituzionale, sentenza n. 170 del 5 giugno 1984 secondo cui: "*La Corte costituzionale dichiara inammissibile la questione di legittimità costituzionale dell'art. 3 del d.P.R. 22 settembre 1978, n. 6955 sollevata con l'ordinanza in epigrafe dal Tribunale di Genova in riferimento all'art. 11 Cost. e in relazione agli artt. 177 e 189 del Trattato di Roma*"
http://leg15.camera.it/cartellecomuni/leg14/RapportoAttivitaCommissioni/commissioni/allegati/14/14_all_1984170sentc.pdf

Corte costituzionale svolge un ruolo cruciale non solo nel garantire i diritti fondamentali attraverso sentenze che annullano leggi incostituzionali, ma anche nel contribuire allo sviluppo e all'espansione dei principi fondamentali enunciati nella Costituzione.

In questo contesto, la Costituzione riconosce e garantisce i diritti inviolabili dell'uomo, sia individualmente che nelle comunità in cui si realizza. La Corte costituzionale chiarisce che il suo ruolo è quello di proteggere i diritti esistenti e di adattarsi alle nuove esigenze emergenti nella società moderna. La Corte costituzionale è chiamata a bilanciare i valori costituzionali in conflitto quando si tratta di diritti di diversa natura e importanza. Questo equilibrio è cruciale per garantire che l'esercizio di un diritto fondamentale non comprometta altri interessi o diritti di pari rilevanza.

La libertà di manifestazione del pensiero è considerata sia un diritto fondamentale per l'individuo, sottolineando -ancora- il principio personalistico, sia un elemento essenziale per il funzionamento corretto della democrazia. Importanti principi in proposito sono stati affermati dalla sentenza della Corte costituzionale, la n. 86 del 1974[67], che ha affrontato il tema del bilanciamento dei valori sanciti dalla Costituzione. In tale sentenza si afferma che il diritto costituzionalmente garantito di esprimere liberamente il proprio pensiero non comporta una protezione assoluta e illimitata della libertà di espressione, poiché ci sono dei limiti imposti dal dovere di preservare gli altrui diritti e di tutelare altri beni o interessi altrettanto riconosciuti e difesi dalla Costituzione. Tra questi, l'onore (che include decoro e reputazione) è un bene di particolare rilevanza, in quanto è strettamente legato alla dignità umana. Questa affermazione si collega a quanto espresso nella sentenza n. 11 del 1968[68], che sottolinea che il diritto di esprimere liberamente il proprio pensiero attraverso la parola, la scrittura e altri mezzi di diffusione è intrinseco al regime di libertà garantito dalla

[67] Sentenza Corte costituzionale n. 86 del 1974
https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:1974:86

[68] Sentenza Corte costituzionale n. 11 del 1968.
https://www.cortecostituzionale.it/actionSchedaPronuncia.do?param_ecli=ECLI:IT:COST:1968:11

Costituzione e non può essere limitato da norme che aprano la strada a pericolose minacce. Non esiste alcun interesse pubblico che possa giustificare restrizioni non autorizzate dalla Costituzione stessa. La Corte costituzionale ha anche affrontato il tema della dignità umana in relazione a diversi diritti e libertà, tra cui la salute, la libertà personale, la coscienza individuale e l'ambiente. Questi diritti sono considerati parte integrante della dignità umana e devono essere protetti in modo da non limitare irragionevolmente le opportunità di espressione e sviluppo della coscienza individuale.

È dunque chiaro come la Corte costituzionale ha nel tempo sottolineato la necessità di una interpretazione costituzionale orientata verso una giurisprudenza evolutiva che tenga conto dei cambiamenti sociali e culturali. Questo approccio "attualizzato" garantisce che i principi fondamentali della Costituzione italiana siano applicati in modo efficace e appropriato alla società contemporanea. La Corte costituzionale è sempre più chiamata a dirimere conflitti tra diversi diritti. Ad esempio, si pensi alle situazioni in cui si verificano conflitti tra il diritto alla privacy e il diritto all'informazione; tra il diritto al lavoro e il diritto all'iniziativa economica; tra il diritto di proprietà e la sua funzione sociale, o ancora tra la libertà di iniziativa economica e il diritto all'ambiente, oltre che tra la libertà personale e la necessità di garantire la libera circolazione delle informazioni.

Tornando alla nostra materia, l'attenzione necessaria per proteggere i dati personali spesso porta a trascurare il secondo aspetto importante del GDPR, che è la libera circolazione delle informazioni all'interno dell'Unione europea. Questo principio è sancito nel Considerando n. 5 del GDPR[69], dove si stabilisce che le autorità nazionali degli Stati membri dell'Unione devono collaborare e

[69] GDPR Considerando n. 5: "*L'integrazione economica e sociale conseguente al funzionamento del mercato interno ha condotto a un considerevole aumento dei flussi transfrontalieri di dati personali e quindi anche dei dati personali scambiati, in tutta l'Unione, tra attori pubblici e privati, comprese persone fisiche, associazioni e imprese. Il diritto dell'Unione impone alle autorità nazionali degli Stati membri di cooperare e scambiarsi dati personali per essere in grado di svolgere le rispettive funzioni o eseguire compiti per conto di un'autorità di un altro Stato membro.*"

condividere dati personali per svolgere le rispettive funzioni o compiti per conto di un'autorità di un altro Stato membro. Questo principio può essere collegato alla disciplina delle informazioni non personali prevista nella Direttiva "Open Data", che promuove il riutilizzo delle informazioni del settore pubblico, nota come Direttiva n. 2019/1024[70]. Questi due atti normativi tipici fanno parte di un ampio processo legislativo europeo volto a proteggere i consumatori e promuovere la concorrenza nel contesto della strategia per il mercato unico digitale. L'obiettivo è rendere l'Unione europea e lo Spazio Economico Europeo più competitivi attraverso il trattamento "*corretto*" e "*lecito*" dei preziosi "*dati*", consentendo loro di stare al passo con il mercato globale.

Il GDPR mette al centro della sua protezione l'individuo, la sua dignità, la sua autodeterminazione informativa e le sue libertà fondamentali. Questi aspetti devono essere preservati per garantire una rappresentazione accurata di sé stessi attraverso la propria immagine e le informazioni riferibili a sé. Tuttavia, il Legislatore europeo non si è limitato a incrementare il controllo dell'individuo sui propri dati, ma ha anche voluto promuovere la libera circolazione dei dati per stimolare l'economia digitale. Tra gli strumenti previsti per facilitare la circolazione dei dati, rientra la previsione del diritto alla portabilità dei dati, che, consentendo il trasferimento agevole di dati personali da un servizio online ad un altro, mira a favorire la concorrenza tra le imprese, promuovere l'innovazione e sviluppare nuovi servizi. In questo modo, un individuo può spostare facilmente un contratto di servizi da un fornitore a un altro senza dover fornire nuovamente tutti i propri dati, chiedendo semplicemente al fornitore precedente di trasferire i dati al nuovo fornitore.

L'articolo 20 del GDPR[71] stabilisce infatti che l'individuo ha il diritto, se i dati personali sono trattati in modo automatizzato, di ricevere tali dati in un formato strutturato, comunemente usato e leggibile da dispositivi automatici, per trasmetterli a un altro responsabile del trattamento. Pertanto, il Regolamento

[70] Direttiva (UE) 2019/1024 del Parlamento europeo e del Consiglio del 20 giugno 2019 relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico (rifusione).

[71] GDPR art. 20 - Diritto alla portabilità dei dati

promuove lo sviluppo di formati interoperabili che agevolino la portabilità dei dati. In sintesi, il diritto alla portabilità dei dati ha due obiettivi principali:

1) aumentare il controllo dell'individuo sui propri dati, consentendo di accedervi e riceverli in un formato facilmente leggibile e utilizzabile;
2) agevolare il trasferimento dei dati a un altro responsabile del trattamento, anche attraverso l'uso di formati standard per semplificare questo processo.

Tuttavia, la questione è assai articolata e il dibattito resta aperto: il diritto alla portabilità dei dati è ancora in fase di sviluppo e presenta sfide, in parte perché molti utenti non ne hanno ancora compreso appieno le utilità pratiche e in parte perché il GDPR non fornisce indicazioni specifiche sul formato dei dati da trasferire, soprattutto considerando le differenze tra i settori di attività.

Negli ultimi anni una nuova prospettiva chiave si è imposta, quella del valore economico dei dati personali. La questione è particolarmente significativa nell'ambito dei servizi digitali, poiché spesso gli utenti sono chiamati a decidere se condividere i propri dati personali in cambio di servizi gratuiti o, in alternativa, di un abbonamento a pagamento. Questo concetto ha portato a riflettere sul fatto che implicitamente si attribuisce un valore economico ai dati personali quando si offre l'opzione di acconsentire al trattamento in cambio di servizi gratuiti. Nel mondo digitale odierno, servizi, applicazioni[72] e piattaforme online sono diventati una parte essenziale della vita quotidiana. Molte di queste piattaforme offrono servizi gratuiti, come social media, e-mail, servizi di messaggistica e molto altro, ma spesso chiedono in contropartita l'autorizzazione per raccogliere, elaborare e utilizzare i dati personali dell'utente. Questa pratica ha generato il detto comune secondo cui "…*quando un servizio è gratuito, la merce sei tu*." In altre parole, il servizio offerto gratuitamente è

[72] Applicazione per apparecchi elettronici tipo PC, tablet PC, smartphone ecc. - Garzanti Linguistica https://www.garzantilinguistica.it/ricerca/?q=app

sostenuto dalla raccolta e dalla "monetizzazione"[73] dei dati personali dell'utente. Le organizzazioni utilizzano spesso i dati personali per scopi di marketing, pubblicità mirata e analisi dei consumatori e questi dati possono essere utilizzati per creare profili dettagliati degli utenti, consentendo alle aziende di adattare le loro strategie di marketing e pubblicità in base ai comportamenti e alle preferenze degli utenti. Questo *targeting* mirato (profilazione) è altamente prezioso per le aziende, poiché aumenta l'efficacia delle loro campagne pubblicitarie e può portare a un aumento dei profitti.

Di conseguenza, è emerso il moderno tema del delicato equilibrio tra il valore economico dei dati e la protezione della privacy degli utenti e, conseguentemente, sono nati nuovi interrogativi e dibattiti sul corretto bilanciamento tra la protezione del diritto fondamentale alla privacy e la promozione dello sviluppo di nuovi servizi necessari per garantire la pluralità e la competitività del mercato unico digitale.

Per affrontare queste sfide, il Garante per la protezione dei dati personali (di seguito il Garante)[74], ha coinvolto il Comitato europeo per la protezione dei dati[75] per cercare di stabilire un orientamento condiviso in ambito europeo, al fine di garantire un'applicazione uniforme delle normative vigenti.

---

[73] Monetizzare: trasformare in guadagno economico una situazione di vantaggio, Considerare un bene o un servizio in base al suo equivalente monetario, Vocabolario Treccani https://www.treccani.it/vocabolario/monetizzare/

[74] Il Garante per la protezione dei dati personali è un'autorità amministrativa indipendente istituita dalla cosiddetta legge sulla privacy (legge 31 dicembre 1996, n. 675), poi disciplinata dal Codice in materia di protezione dei dati personali (Decreto Legislativo 30 giugno 2003 n. 196), come modificato dal Decreto Legislativo del 10 agosto 2018, n. 101. Quest'ultimo ha confermato che il Garante è l'autorità di controllo designata anche ai fini dell'attuazione del Regolamento generale sulla protezione dei dati personali (UE) 2016/679 (art. 51).
https://www.garanteprivacy.it/home/autorita

[75] Comitato europeo per la protezione dei dati (EDPB) è un organismo europeo indipendente. È l'organizzazione sotto la cui egida si riuniscono le Autorità nazionali per la protezione dei dati personali (Autorità nazionali di controllo) dei paesi dello Spazio economico europeo, nonché il Garante europeo della protezione dei dati (EDPS).

Con riguardo al tema dello sviluppo di nuovi servizi, merita un approfondimento la questione degli "Open Data"[76], o dati aperti. Si tratta di informazioni accessibili a chiunque, fornite da enti pubblici o aziende private, che possono essere riutilizzate per vari scopi, come ad esempio i dati della PA, dati scientifici, ambientali o meteorologici, ecc. La normativa relativa agli open data ha avuto origine nel 2003[77] e ha subito una significativa revisione nel 2013[78]. Inoltre, è stata ulteriormente modificata, come già anticipato, nel giugno 2019[79], tenendo conto dei cambiamenti tecnologici e sociali avvenuti negli ultimi cinque anni e integrando le direttive sulla gestione dei dati. Attraverso gli Open Data, le imprese possono trarre vantaggio dai dati detenuti dalle pubbliche amministrazioni al fine di migliorare i propri modelli di business o svilupparne di nuovi. L'Unione europea ha previsto che l'aumento della disponibilità di dati aperti forniti dai 27 Paesi membri[80] possa generare notevoli benefici economici nei prossimi anni, creando allo stesso tempo nuovi posti di lavoro nel settore dell'analisi dei dati. Inoltre, l'accesso libero alle informazioni pubbliche da parte di tutti può promuovere la trasparenza, migliorare la qualità del dibattito sulle politiche pubbliche e rendere più efficiente l'amministrazione pubblica.

È importante notare che, in linea con la normativa sulla protezione dei dati personali, gli Open Data non includono documenti contenenti dati personali il cui riutilizzo sia incompatibile con gli scopi originali del trattamento da parte delle Pubbliche Amministrazioni. Questo significa che i dati personali non possono essere considerati Open Data, a meno che esista una legge che autorizzi o

[76] Cosa sono gli Open Data e a cosa servono, forumpa.it, testata online di FPA https://www.forumpa.it/pa-digitale/open-data-cosa-sono-come-sfruttarli-e-stato-dellarte-in-italia/

[77] Direttiva 2003/98/CE del Parlamento europeo e del Consiglio relativa al riutilizzo dell'informazione del settore pubblico.

[78] Direttiva 2013/37/CE del Parlamento europeo e del Consiglio che modifica la direttiva 2003/98/CE relativa al riutilizzo dell'informazione del settore pubblico.

[79] Direttiva UE 2019/1024 del Parlamento europeo e del Consiglio relativa all'apertura dei dati e al riutilizzo dell'informazione del settore pubblico.

[80] Unione europea, profili dei Paesi https://european-union.europa.eu/principles-countries-history/country-profiles_it

imponga la loro pubblicazione, o sia stato ottenuto il consenso per la diffusione dei dati. Al riguardo, il Data Governance Act[81] è una recentissima norma dell'Unione europea, in vigore dal 24 settembre 2023, con l'obiettivo principale di promuovere la libera circolazione dei dati e creare fiducia negli scambi di dati. È nato dunque il primo Regolamento sui dati approvato nel contesto della strategia sui dati dell'Unione europea, che si pone in continuità e in un rapporto di complementarità con il GDPR poiché mira a garantire che i dati personali siano trattati in modo sicuro e conforme alle leggi sulla privacy, mantenendo al contempo il focus sulla libera circolazione dei dati e la promozione di condizioni di sicurezza e libera concorrenza negli scambi di dati. Questi due Regolamenti lavorano sinergicamente per proteggere i diritti degli individui e promuovere lo sviluppo dello spazio digitale in Europa.

Per quanto riguarda i dati personali e tornando al GDPR, è fondamentale riconoscere che la principale finalità della norma è la protezione dei dati tramite il rispetto dei principi generali indicati nell'articolo 5[82]. Tra questi si evidenzia il principio dell'esattezza e dell'aggiornamento dei dati personali. Ogni operazione e analisi dei dati deve rispettare e promuovere il benessere delle persone fisiche e contribuire al progresso economico e sociale del mercato europeo, ma questo può accadere solo se si basa su dati accurati, pertinenti e aggiornati. Pertanto, è sempre più importante comprendere che la protezione e la libera circolazione dei dati devono essere fondate su basi di dati solide e verificabili.

L'equilibrio tra la protezione dei diritti fondamentali e la libera circolazione delle informazioni è un tema centrale nell'era digitale. Da un lato, si avverte la necessità di proteggere la privacy, la dignità umana e la libertà di espressione, che sono diritti fondamentali garantiti dalle leggi nazionali e internazionali. Dall'altro lato, non può essere trascurata la crescente importanza della libera circolazione dei dati, che promuove l'innovazione, l'efficienza economica e la trasparenza. La protezione dei dati personali è fondamentale per garantire che

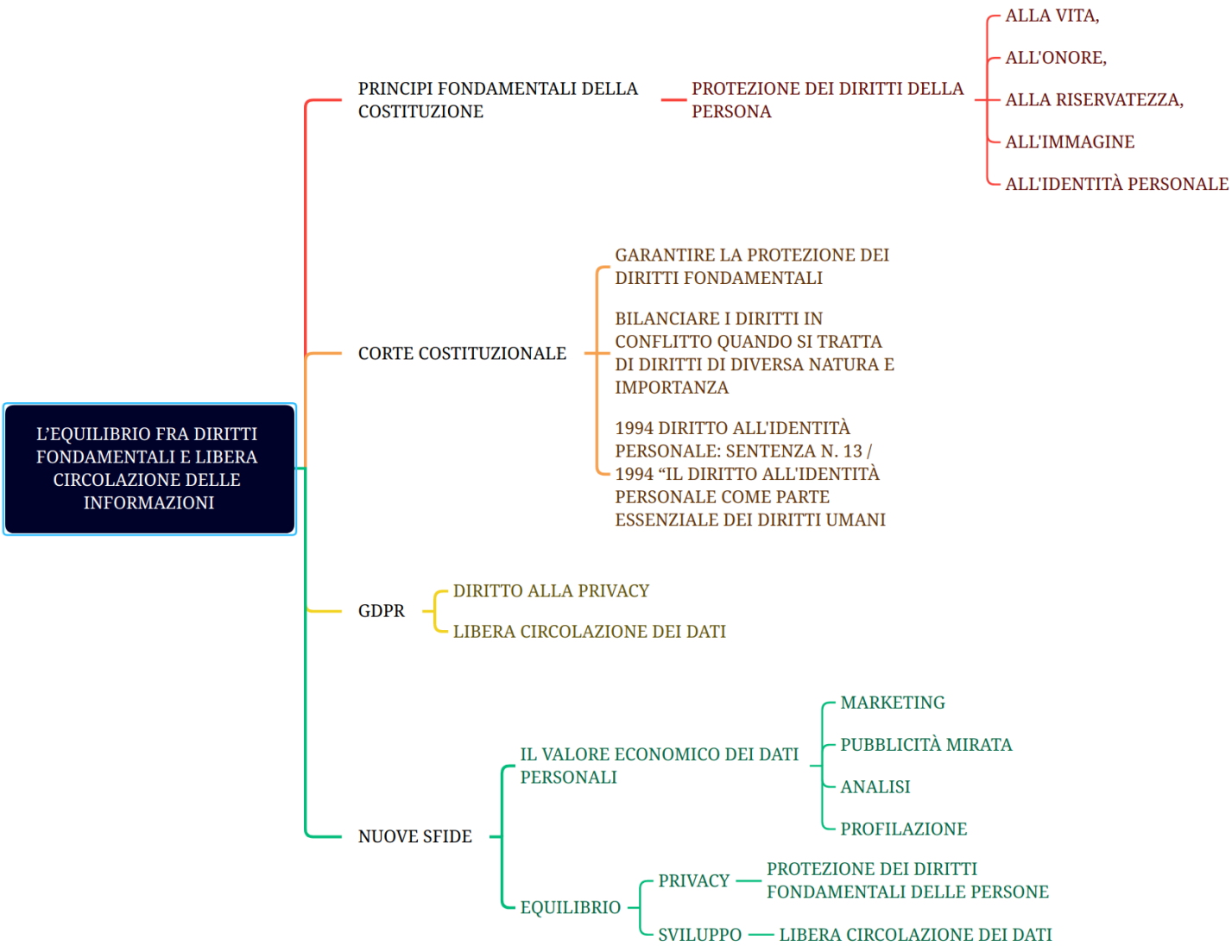
[81] Commissione europea, European Data Governance Act https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

[82] GDPR art. 5 - Principi applicabili al trattamento di dati personali

le persone mantengano il controllo sulle informazioni che riguardano la loro vita. È importante stabilire limiti chiari sul trattamento dei dati personali e richiedere il consenso quando necessario. Inoltre, il principio di esattezza e aggiornamento dei dati è essenziale per garantire che i dati siano affidabili e pertinenti. Tuttavia, la libera circolazione delle informazioni, inclusi i sopracitati Open Data, può portare a benefici significativi per la società: le imprese possono utilizzare queste informazioni per migliorare i propri servizi o svilupparne di nuovi od innovare; il libero accesso alle informazioni pubbliche può promuovere la trasparenza e migliorare la qualità del servizio pubblico. Il bilanciamento tra questi due obiettivi non è un compito facile. È importante sviluppare standard interoperabili che consentano il trasferimento dei dati in modo sicuro e consentano alle persone di spostare i propri dati da un servizio a un altro. Allo stesso tempo, dobbiamo considerare attentamente come trattare i dati personali in modo responsabile, evitando abusi o violazioni della privacy.

Inoltre, dobbiamo essere consapevoli che questo equilibrio non è fisso ma in evoluzione, che la tecnologia cambia e la società evolve, e che quindi anche le leggi e le normative devono adattarsi. Questo processo richiede il coinvolgimento di diverse parti interessate, compresi governi, aziende, organizzazioni della società civile e individui. È un equilibrio che va cercato costantemente, considerando sia gli interessi delle persone che quelli della società nel loro complesso. L'obiettivo ambizioso è creare una società digitale equa, sicura ed efficiente in cui le persone possano godere dei vantaggi delle nuove tecnologie senza compromettere i loro diritti e la loro dignità.

Mappa concettuale 6 – L’equilibrio fra diritti fondamentali e libera circolazione delle informazioni



Capitolo Terzo - L'accountability

Il principio generale

L'accountability è un termine inglese che si traduce in italiano con il termine "*responsabilizzazione*". Esso è un principio fondamentale nell'ambito della governance dell'amministrazione pubblica e delle organizzazioni in generale e si è andato diffondendo sempre più negli ultimi anni. Volendo darne una definizione, con accountability ci si riferisce alla responsabilità e alla trasparenza delle azioni e delle decisioni prese da individui o entità, e alla loro capacità di essere responsabili del loro agire. Tale principio, dunque, rappresenta un elemento chiave per garantire che le azioni e le decisioni siano prese in modo responsabile e trasparente, e che coloro che agiscono al di fuori dei parametri stabiliti siano tenuti responsabili delle loro azioni. È un concetto recente e moderno, che trova ispirazione nel paradigma di governance del "*New Public Management*"[83], cruciale in molti aspetti dalla governance pubblica, ma anche delle organizzazioni private, che gioca un ruolo essenziale nell'assicurare la fiducia e il funzionamento efficace della società, attraverso le istituzioni.
Elemento fondamentale dell'accountability è la trasparenza, che implica che le azioni e le decisioni debbano essere chiaramente visibili e comprensibili da parte del pubblico e/o degli stakeholder interessati; può riguardare la divulgazione di informazioni finanziarie, politiche o operative. Ne deriva che le persone, in primo luogo, e le organizzazioni di conseguenza, dovranno essere in grado di rispondere del loro operato, di decisioni e di azioni, incappando altrimenti in sanzioni o obblighi di riparazione. L'accountability implica anche la possibilità di monitorare e valutare le azioni e le prestazioni scelte e ciò può essere fatto attraverso audit, revisioni, valutazioni o altri mezzi di controllo che verificano

[83] Rivista Italiana di Public Management, Public Management: una prospettiva di scienza dell'organizzazione.
https://www.rivistaitalianadipublicmanagement.it/miglioramento-dei-processi-di-attuazione-degli-interventi-in-materia-di-edilizia-scolastica/

l'aderenza alle norme o agli standard stabiliti. Inoltre, coinvolgere le parti interessate nella presa di decisioni è un aspetto importante dell'accountability e questo contribuisce a garantire che le decisioni siano prese in modo equo e che gli interessi delle diverse parti siano presi in considerazione.
Norme, leggi e regolamenti svolgono un ruolo chiave nell'assicurare l'accountability, forniscono le basi su cui valutare le azioni e stabiliscono le conseguenze per le violazioni.
Con l'avanzare della tecnologia, l'accountability si estende anche all'ambito digitale: la protezione dei dati personali, la sicurezza informatica e la responsabilità per l'uso dell'intelligenza artificiale sono solo alcuni esempi di come la tecnologia ha ampliato la sfera dell'accountability. In ultimo, l'assenza di accountability può portare a comportamenti irresponsabili, corruzione e abusi di potere e per questo essa è fondamentale in molti contesti per garantire la fiducia del pubblico e il funzionamento efficace delle istituzioni.

L'accountability nel GDPR

Il GDPR mette in forte evidenza l'importanza della accountability di titolari e responsabili del trattamento dei dati, vale a dire, l'adozione di azioni proattive che dimostrino concretamente l'attuazione delle misure necessarie per garantire la conformità al Regolamento[84]. Questo rappresenta un notevole cambiamento nel campo della protezione dei dati, poiché affida ai responsabili del trattamento il compito di definire in modo autonomo le modalità, le garanzie e i limiti del trattamento dei dati personali, sempre nel rispetto delle normative e seguendo alcuni criteri specifici stabiliti dal Regolamento.

[84] GDPR art. 23 - Limitazioni, art. 25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita e Capo IV - Titolare del trattamento e responsabile del trattamento.

Il primo di questi criteri è sintetizzato dall'espressione "*data protection by default and by design*"[85] che sottolinea la necessità di impostare il trattamento sin dalla progettazione iniziale di procedure e sistemi ICT, prevedendo le garanzie essenziali per soddisfare i requisiti del Regolamento e proteggere i diritti degli interessati. Questo, evidentemente, deve ora essere fatto in anticipo, ossia deve iniziare prima di effettuare il trattamento dei dati, e deve ovviamente continuare per tutta la durata del trattamento, come specificato nell'articolo 25 del GDPR. Ciò richiede quindi un'analisi preventiva e uno sforzo da parte dei responsabili del trattamento, che devono concretizzarsi in una serie di attività specifiche e dimostrabili.

Tra queste attività, rivestono un ruolo fondamentale quelle relative al criterio stabilito dal Regolamento riguardo alla gestione degli obblighi dei responsabili, ovvero il rischio associato al trattamento. Questo rischio si riferisce agli impatti negativi sulle libertà e i diritti degli interessati[86]. Tali impatti devono essere

[85] GDPR art. 25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita.

[86] GDPR - Considerando n. 75: *"I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati*" e considerando 77 "*Gli orientamenti per la messa in atto di opportune misure e per dimostrare la conformità da parte del titolare del trattamento o dal responsabile del trattamento in particolare per quanto riguarda l'individuazione del rischio connesso al trattamento, la sua valutazione in termini di origine, natura, probabilità e gravità, e l'individuazione di migliori prassi per attenuare il rischio, potrebbero essere forniti in particolare mediante codici di condotta approvati, certificazioni approvate, linee guida fornite dal*

considerati attraverso un processo di valutazione dedicato[87], prendendo in considerazione i rischi noti o prevedibili e le misure tecniche e organizzative (anche di sicurezza) che il responsabile del trattamento ritiene necessarie per mitigare questi rischi. Al termine di questa valutazione di impatto, il responsabile del trattamento può decidere autonomamente se iniziare il trattamento (avendo adottato misure sufficienti per mitigare il rischio) o se consultare l'Autorità nazionale di controllo per ottenere indicazioni su come gestire il rischio residuale. Il Garante -si badi, sempre in virtù del principio di accountability- non ha il compito di "autorizzare" il trattamento, ma di fornire indicazioni sulle eventuali misure correttive da adottare[88] ed eventualmente intervenire con azioni che possono variare dall'ammonizione del responsabile del trattamento fino alla limitazione o al divieto di effettuare il trattamento. L'approccio innovativo, dunque, è rappresentato dal fatto che l'intervento delle autorità di controllo avviene principalmente in una fase "ex post", cioè dopo che il titolare ha preso autonomamente le decisioni necessarie in base alle sue competenze ed esperienza. Non occorrerà più alcuna notifica preventiva all'autorità di controllo, né il cosiddetto "prior checking" per la verifica preliminare.

Alle autorità di controllo, in particolare al Comitato europeo per la protezione dei dati, è affidato un ruolo di "*garante*" di un approccio corretto ed uniforme al trattamento. Il Garante per la protezione dei dati personali ha un ruolo cruciale nell'assicurare che le leggi sulla privacy e il GDPR siano adeguatamente applicati nel nostro Paese. Questa Autorità svolge diverse attività, tra cui la verifica della conformità dei trattamenti dei dati personali alle leggi vigenti e al Regolamento. In caso di una non conformità, il Garante può imporre misure correttive ai titolari dei dati o ai responsabili del trattamento. Inoltre, il Garante collabora con le altre autorità di controllo europee per una coerente applicazione delle leggi sulla

comitato o indicazioni fornite da un responsabile della protezione dei dati. Il comitato può inoltre pubblicare linee guida sui trattamenti che si ritiene improbabile possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche e indicare quali misure possono essere sufficienti in tali casi per far fronte a tale rischio".

[87] GDPR art. 35 - Valutazione d'impatto sulla protezione dei dati, art. 36 - Consultazione preventiva

[88] GDPR art. 58 - Poteri

privacy, cosa particolarmente importante in un contesto internazionale in cui i dati personali possono attraversare le frontiere. Il Garante esamina anche i reclami presentati dai cittadini in merito alla protezione dei loro dati personali e interviene quando vi sono violazioni delle normative. Un aspetto significativo del ruolo del Garante è il monitoraggio delle attività delle autorità pubbliche e private che trattano dati personali. Questo monitoraggio può comportare l'emissione di avvertimenti, divieti o altre misure preventive e correttive per garantire la tutela dei diritti delle persone. Si tratta di un ruolo essenziale nell'assicurare che coloro che trattano dati personali siano responsabilizzati.

I titolari ed i responsabili del trattamento devono adottare misure preventive per garantire la conformità alla pertinente disciplina; il Garante interviene in caso di presunte violazioni, esaminando le situazioni e, se necessario, imponendo sanzioni e divieti. In questo modo, il rispetto dell'accountability da parte dei titolari responsabili del trattamento viene rigorosamente verificata. Naturalmente al Garante sono attribuiti anche compiti di informazione e formazione, con l'obiettivo di far conoscere al pubblico ed ai titolari del trattamento i loro diritti e doveri. Inoltre, il Garante tiene registri delle violazioni più gravi delle normative sulla privacy e può imporre sanzioni pecuniarie quando necessario, che hanno il fine di dissuadere comportamenti non conformi e garantire il rispetto delle leggi.

Infine, il Garante può coinvolgere i cittadini e altri soggetti interessati nelle questioni che riguardano la protezione dei dati attraverso consultazioni pubbliche. Questo processo consente di tener conto delle opinioni e delle preoccupazioni delle persone nella formulazione delle politiche sulla privacy.

Tornando alle responsabilità dei titolari e dei responsabili del trattamento dei dati personali, il GDPR presenta alcune importanti ulteriori innovazioni che promuovono un approccio più responsabilizzante nei confronti della gestione dei dati personali. Innanzitutto, vi è in alcuni casi l'obbligo di mantenere un registro

dei trattamenti[89]. Questo non è solo un obbligo formale, ma un elemento essenziale di un sistema di gestione adeguato dei dati personali. Il registro fornisce una panoramica chiara di tutti i trattamenti in corso all'interno di un'organizzazione ed è fondamentale per la valutazione dei rischi. Anche se il GDPR esclude dall'obbligo le organizzazioni con meno di 250 dipendenti che non trattano dati ad alto rischio, è sempre consigliabile (ai fini dell'accountability, appunto) tenere un registro completo.

Le misure di sicurezza devono essere proporzionate al rischio di trattamento dei dati; non esiste una lista predefinita di misure, ma esse devono essere adeguate alle specifiche circostanze di ciascun trattamento:

> "*…il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio"*[90]*.*

Questa flessibilità consente da un lato di personalizzare in autonomia le misure di sicurezza in base ai rischi specifici che gli addetti sapranno ben valutare, ma rappresenta al tempo stesso il cardine del nuovo principio di accountability, ovvero il criterio della "*adeguatezza*" riferito dapprima alle misure, poi al rischio ed alla sicurezza. Questo rappresenta l'enorme passo avanti compiuto dal Legislatore europeo rispetto ai requisiti minimi di sicurezza previsti dal vecchio Codice della Privacy.

Altro elemento innovativo correlato all'accountability è rappresentato dalle notifiche delle violazioni: i titolari sono tenuti a notificare all'autorità di controllo eventuali violazioni dei dati personali entro 72 ore dalla loro scoperta, e in ogni caso senza ritardi non giustificati. La notifica non è obbligatoria; essa è richiesta

---

[89] GDPR art. 30 - Registri delle attività di trattamento: Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda art. 30, paragrafo 5: "*Gli obblighi di cui ai paragrafi 1 e 2 non si applicano alle imprese o organizzazioni con meno di 250 dipendenti, a meno che il trattamento che esse effettuano possa presentare un rischio per i diritti e le libertà dell'interessato, 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*"), devono tenere un registro delle operazioni di trattamento.

[90] GDPR art. 32 - Sicurezza del trattamento

solo se si ritiene probabile che la violazione possa comportare rischi per i diritti e le libertà delle persone coinvolte. Anche la decisione di notificare una violazione (o di non farlo) all'autorità è basata sulla auto-valutazione del rischio per gli interessati, il che -di nuovo- prevede che se ne assumano la responsabilità i titolari. Se il rischio è considerato significativo, questi ultimi devono anche informare tempestivamente gli interessati sulla violazione. Va precisato che esistono alcune eccezioni a questa regola[91]. I dettagli specifici relativi al contenuto delle notifiche all'autorità e delle comunicazioni agli interessati sono definiti in modo specifico[92].

Come già anticipato, la nomina del "*responsabile della protezione dei dati*" (RPD), più noto con l'acronimo inglese DPO (Data Protection Officer), è un altro aspetto che riflette l'approccio di responsabilizzazione sostenuto dal GDPR. Questo ruolo è stato creato per agevolare l'implementazione del Regolamento da parte dei titolari del trattamento e dei responsabili. È interessante notare che tra le responsabilità del DPO vi è quella di sensibilizzare e formare il personale dell'organizzazione, nonché di supervisionare la valutazione d'impatto[93]. La nomina del DPO è obbligatoria in alcuni casi specifici[94], e richiede che esso risponda a specifici prerequisiti sia in termini di indipendenza, imparzialità e riservatezza (anche al fine di evitare conflitti d'interessi), che di competenze specifiche[95].

L'analisi condotta ha dunque evidenziato come il GDPR preveda l'approccio basato sull'elasticità e dunque spingendo le organizzazioni a gestire in modo proattivo i dati personali e ad adottare in autonomia misure adeguate (ivi comprese quelle relative alla sicurezza[96]) di protezione in funzione del settore di

[91] GDPR art. 34 - Comunicazione di una violazione dei dati personali all'interessato

[92] GDPR art. 33 - Notifica di una violazione dei dati personali all'autorità di controllo, art. 34 - Comunicazione di una violazione dei dati personali all'interessato

[93] GDPR art. 35 - Valutazione d'impatto sulla protezione dei dati

[94] GDPR art. 37 - Designazione del responsabile della protezione dei dati

[95] GDPR art. 38 - Posizione del responsabile della protezione dei dati, art. 39 - Compiti del responsabile della protezione dei dati

[96] GDPR art. 32 - Sicurezza del trattamento

mercato, della tipologia e dell'attività d'impresa, delle dimensioni, della tipologia di prodotti o servizi offerti, ecc.

"*Il GDPR è informato da un generale* "principio di elasticità*" in base al quale gli obblighi si comprimono od espandono al massimo a seconda del rischio e gravità correlati al trattamento dei dati e della struttura organizzativa: lascia dunque maggiore discrezionalità al Titolare del trattamento nel decidere attraverso quali modalità "adeguate" tutelare i dati -modello operativo flessibile- abbandonando ad esempio il concetto generale ed astratto -modello operativo rigido- di misure minime di sicurezza e di precetti vincolati con scadenze e adempimenti indifferenziati per tutti i destinatari dell'obbligo."*[97]

Tuttavia, questa estremizzazione dell'autonomia e della flessibilità può comportare un rischio di sottovalutazione da parte delle organizzazioni, che potrebbero non percepire immediatamente la gravità delle conseguenze legate alla non conformità. Dunque, se da un lato è stato introdotto un approccio flessibile e di tolleranza basato anche sulla fiducia, dall'altro le organizzazioni sono chiamate ad una maggior consapevolezza dei rischi legati alla eventuale non conformità. Il principio di accountability è fondamentale in tutto il GDPR, permeando ogni aspetto della sua struttura. Questo principio richiede una revisione ed un costante aggiornamento dei processi delle organizzazioni. I titolari del trattamento dei dati devono periodicamente riesaminare e aggiornare le misure di sicurezza, attualizzando la valutazione di impatto ogni volta che sorgono nuove variazioni di rischio per garantire in modo continuo la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi tecnologici e molto altro.

In aggiunta, è essenziale comprendere che la protezione dei dati personali è un campo in costante evoluzione, strettamente legato alle nuove tecnologie. La chiave per valutare la conformità al GDPR risiede nel valutare i rischi per i diritti e le libertà degli interessati. Questi rischi sono di vario tipo e includono situazioni

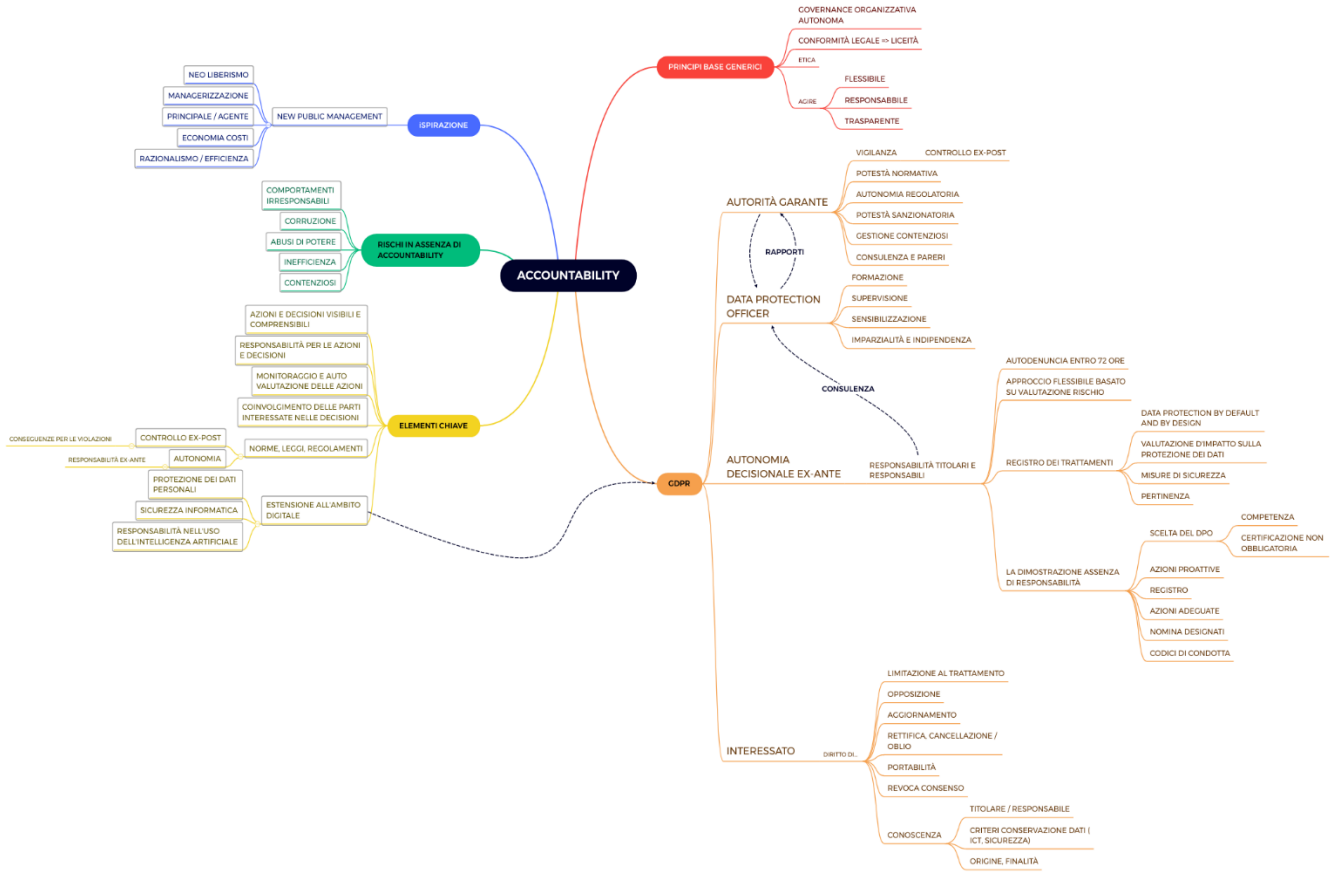
[97] TOSI E., Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale, Milano, 2019, P. 37

come la perdita del controllo dei dati personali, la limitazione dei diritti degli individui, la discriminazione, il furto o l'usurpazione di identità, le perdite finanziarie, la decifratura non autorizzata dei dati, il pregiudizio alla reputazione e il compromesso del segreto professionale, nonché qualunque altro danno economico o sociale significativo per le persone coinvolte.

Per rispettare il principio di accountability, è necessario adottare gli strumenti e le pratiche adatte per implementare misure efficaci, che possono includere ad esempio la creazione di procedure per l'identificazione di tutte le operazioni di trattamento dei dati, la pronta risposta alle richieste di accesso ai dati da parte degli interessati, l'allocazione di risorse adeguate e la designazione di individui responsabili per garantire la conformità alla protezione dei dati. Inoltre, la gestione dinamica del registro dei trattamenti è essenziale per tenere traccia di tutte le attività di trattamento dei dati.

L'espansione delle nuove tecnologie e la crescente globalizzazione dell'economia e della società hanno portato a una massiccia proliferazione di dati personali, di conseguenza i rischi connessi a questi dati si sono moltiplicati in modo significativo. L'aumento dei rischi e del valore dei dati personali richiede un approccio proattivo e dinamico da parte dei titolari del trattamento, che devono identificare e applicare misure adeguate ed efficaci per garantire la conformità al GDPR. Questo sforzo richiede anche la promozione di una cultura delle organizzazioni basata sulla consapevolezza e la comprensione delle sfide legate alla protezione dei dati personali. Fondamentali sono gli investimenti nella formazione e nelle tecnologie, sino al ricorso a consulenze tecniche e legali quando necessario. La protezione dei dati personali non deve essere vista solo come un obbligo legale, bensì come un investimento nella sicurezza, nella reputazione e nella sostenibilità a lungo termine dell'organizzazione.

Mappa concettuale 7 – L’accountability



Capitolo Quarto - La responsabilità civile da illecito trattamento dei dati personali

La tutela rimediale

Per garantire la tutela dei diritti individuali relativi al trattamento dei dati personali, chi ritiene che i diritti di cui gode in base alla normativa in materia di tutela dei dati personali siano stati violati, può percorrere due strade alternative:

a) rivolgersi all'autorità di controllo preposta, ovvero al Garante (eventualmente passando prima per un'istanza diretta al titolare del trattamento);
b) utilizzare gli strumenti di tutela giurisdizionale, ovvero rivolgersi al giudice ordinario.

Nell'elaborato si esploreranno in particolare i rimedi privatistici che le persone fisiche possono adottare quando si trovano di fronte a una violazione dei loro diritti in materia di dati personali; senza entrare troppo nel merito delle sanzioni amministrative o penali, tipiche del diritto pubblico, ancorché va osservato che quest'ultime rappresentano il principale deterrente per il rispetto delle norme sulla protezione dei dati. Infatti, è importante sottolineare che, nella pratica, le norme sulla protezione dei dati personali si basano principalmente su sanzioni amministrative pecuniarie per garantire la loro efficacia.

In molti casi, i rimedi privatistici, che consentono alle persone di chiedere la cessazione delle violazioni dei loro diritti ed eventualmente il risarcimento dei danni subiti, hanno -purtroppo- un'applicazione ristretta. Questo perché spesso le violazioni delle norme sulla protezione dei dati non causano danni significativi o, addirittura, danni tangibili o quantificabili a livello individuale o, semplicemente, sono di difficile dimostrazione in termini di effettiva gravità. Prima di entrare nei dettagli delle norme sulla responsabilità per il trattamento illecito dei dati personali, che possono essere applicate attraverso procedimenti

giudiziari ordinari, è cruciale comprendere il ruolo di un attore chiave nel campo della protezione dei dati: l'autorità di controllo. Quest'ultima svolge un ruolo fondamentale nel monitorare l'applicazione delle norme sulla protezione dei dati e garantire il rispetto dei diritti delle persone fisiche in questo contesto. L'importanza di avere un'autorità di controllo indipendente e imparziale è stata riconosciuta già nella precedente Direttiva 95/46/CE e viene ulteriormente sottolineata come un elemento essenziale per garantire la protezione dei dati personali dalla Carta dei diritti fondamentali dell'Unione europea[98], che stabilisce chiaramente che il rispetto delle regole relative al trattamento dei dati personali deve essere soggetto al controllo di un'autorità indipendente. Questo principio è ribadito nel GDPR, che richiede l'istituzione di una o più autorità pubbliche indipendenti in ciascuno Stato membro. Queste autorità, come già accennato, hanno il compito di sorvegliare sull'applicazione del Regolamento per proteggere i diritti e le libertà fondamentali delle persone fisiche in relazione al trattamento dei dati personali e facilitare la libera circolazione dei dati personali all'interno dell'Unione europea[99]. L'autorità di controllo ha una serie di compiti[100] e poteri[101], tra cui il monitoraggio dell'applicazione delle norme, l'avvio di indagini per accertare le violazioni, l'imposizione di sanzioni e l'adozione di misure correttive. Inoltre, l'autorità di controllo fornisce consulenza e pareri per garantire la corretta applicazione delle norme e affrontano i reclami presentati dagli interessati. Promuove inoltre la consapevolezza pubblica sulle questioni legate alla protezione dei dati personali. L'indipendenza dell'autorità di controllo[102] è fondamentale per assicurare che agisca in modo imparziale e bilanciato. Per garantire questa indipendenza, vengono previste autonomia

[98] Carta dei diritti Fondamentali dell'unione europea art. 8 par. 3 - Protezione dei dati di carattere personale, che al par. 3 afferma: "*Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*"

[99] GDPR art. 51 - Indipendenza, che al par. 1 afferma: "*Ogni autorità di controllo agisce in piena indipendenza nell'adempimento dei propri compiti e nell'esercizio dei propri poteri conformemente al presente regolamento.*"

[100] GDPR art. 57 - Compiti

[101] GDPR art. 58 - Poteri

[102] GDPR art. 62 - Operazioni congiunte delle autorità di controllo

organizzativa, finanziaria e contabile, insieme a norme di incompatibilità per i membri dell'autorità. In Italia, come già affermato, il ruolo di autorità di controllo è affidato al Garante per la protezione dei dati personali[103], un organismo amministrativo indipendente incaricato di supervisionare l'applicazione delle norme sulla protezione dei dati e di proteggere i diritti delle persone fisiche in questo ambito. A livello europeo l'autorità è rappresentata del Garante europeo per la protezione dei dati personali, che supervisiona il trattamento dei dati da parte delle istituzioni dell'Unione europea. Inoltre, le autorità nazionali collaborano con il Garante europeo attraverso il Comitato europeo per la protezione dei dati[104], il cui ruolo principale è assicurare un'applicazione uniforme delle norme sulla protezione dei dati in tutta l'Unione europea e promuovere la cooperazione tra le autorità nazionali. Quando si tratta di trattamenti transfrontalieri, ovvero quando i dati sono trattati in più di uno Stato membro o coinvolgono soggetti interessati in diversi Stati, viene applicato un meccanismo chiamato "sportello unico"[105]. Questo meccanismo designa

[103] Decreto Legislativo 30 giugno 2003, n. 196 recante il "Codice in materia di protezione dei dati personali", Titolo II - Autorità di controllo indipendente, Capo I - Il Garante per la protezione dei dati personali, art. 153 (Garante per la protezione dei dati personali).

[104] GDPR art. 68 - Comitato europeo per la protezione dei dati

[105] GDPR - Considerando n. 127: "*Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila dovrebbe essere competente a trattare casi locali qualora il titolare del trattamento o il responsabile del trattamento sia stabilito in più di uno Stato membro, ma l'oggetto dello specifico trattamento riguardi unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro, ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro. In tali casi, l'autorità di controllo dovrebbe informare senza ritardo l'autorità di controllo capofila sulla questione. Dopo essere stata informata, l'autorità di controllo capofila dovrebbe decidere se intende trattare il caso a norma della disposizione sulla cooperazione tra l'autorità di controllo capofila e altre autorità di controllo interessate («meccanismo dello sportello unico»), ovvero se l'autorità di controllo che l'ha informata debba trattarlo a livello locale. Al momento di decidere se intende trattare il caso, l'autorità di controllo capofila dovrebbe tenere conto dell'eventuale esistenza, nello Stato membro dell'autorità di controllo che l'ha informata, di uno stabilimento del titolare del trattamento o del responsabile del trattamento, al fine di garantire l'effettiva applicazione di una decisione nei confronti del titolare del trattamento o del responsabile del trattamento. Qualora l'autorità di controllo capofila decida di trattare il caso, l'autorità di controllo che l'ha informata dovrebbe avere la possibilità di presentare un progetto di decisione, che*

un'autorità di controllo "*capofila*" responsabile per gestire le questioni relative a tali trattamenti, semplificando il processo per i titolari o i responsabili del trattamento. Per garantire una coerenza nell'applicazione delle norme sulla protezione dei dati in Europa, è stato creato un "meccanismo di coerenza." Questa procedura implica la cooperazione tra le autorità di controllo, il Comitato europeo per la protezione dei dati e, talvolta, la Commissione europea. Ad esempio, in casi importanti, le autorità di controllo nazionali devono consultare il Comitato prima di prendere decisioni, assicurando un approccio coerente. Il Comitato emana linee guida e raccomandazioni che influenzano le decisioni delle autorità di controllo nazionali, contribuendo a una migliore applicazione delle norme sulla protezione dei dati in Europa.

Entrando adesso nel merito degli strumenti di tutela privatistica, come anticipato, le norme prevedono opzioni distinte per gli interessati che ritengono che i propri diritti siano stati violati; queste opzioni sono tre e sono di seguito elencate:

1. istanza al titolare del trattamento (in autonomia) ➔ reclamo al Garante o ricorso al tribunale;
2. reclamo al Garante (tutela amministrativa) ➔ ricorso al tribunale;
3. ricorso al tribunale (tutela giurisdizionale).

In ogni caso, nel complesso, il sistema di tutela in tema di trattamento dei dati personali mira a garantire che gli interessati possano far valere i propri diritti e ottenere rimedi efficaci in caso di violazione delle norme sulla protezione dei dati.

l'autorità di controllo capofila dovrebbe tenere nella massima considerazione nella preparazione del proprio progetto di decisione nell'ambito di tale meccanismo di sportello unico."

La tutela in autonomia

Attraverso l'istanza al titolare del trattamento, un individuo sottoposto a trattamento di dati personali che ritiene che i propri diritti siano stati violati, ha il diritto di inoltrare in autonomia una richiesta direttamente al responsabile del trattamento (o al delegato o tramite un incaricato) senza formalità specifiche, come ad esempio tramite lettera, e-mail, fax, PEC, ecc. Un esempio tipico è la richiesta di cancellare i dati in attuazione del c.d. diritto all'oblio[106] che, ad esempio, può essere presentata direttamente al motore di ricerca come responsabile del trattamento. Il responsabile del trattamento è tenuto a rispondere entro un mese dalla ricezione della richiesta; in casi eccezionali, questo termine può essere esteso a un massimo di tre mesi, ma il responsabile deve comunicare i motivi del ritardo entro il primo mese. Se il responsabile non risponde o la risposta non soddisfa l'interessato, quest'ultimo ha il diritto di rivolgersi all'Autorità di controllo (il Garante per la protezione dei dati) o presentare ricorso direttamente al tribunale.

La tutela amministrativa

Il reclamo presentato al Garante è disciplinato sia dal GDPR[107] che dal codice della privacy (che in realtà rimanda all'art. 77 del GDPR)[108], avviene attraverso uno specifico modulo (modello di reclamo)[109] e rappresenta il passo iniziale che

---

[106] Garante per la Protezione dei Dati Personali, il diritto cosiddetto "*all'oblio" (art. 17 del GDPR) si configura come un diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione.*"
https://www.garanteprivacy.it/i-miei-diritti/diritti/oblio

[107] GDPR art. 77 - Diritto di proporre reclamo all'autorità di controllo

[108] Decreto Legislativo 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*" art. 141 - Reclamo al Garante.

[109] Modello di reclamo https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4535524

gli interessati possono intraprendere quando ritengono che sia avvenuta una violazione dei loro diritti in conformità con le leggi sulla protezione dei dati personali, ovvero una "*violazione dei dati*"[110] (c.d. Data Breach[111]). In confronto all'avvio del ricorso all'autorità giudiziaria, rivolgersi all'autorità di controllo offre notevoli benefici sia in termini di rapidità del procedimento che in termini di riduzione dei costi. Il reclamo al Garante è principalmente incentrato sulla richiesta di misure inibitorie per porre fine alla violazione e garantire il rispetto delle norme sulla protezione dei dati. In altre parole, il Garante può emettere ordini per correggere il comportamento del titolare o del responsabile del trattamento dei dati, se necessario, e può anche decidere di infliggere sanzioni. Se un interessato ha presentato un reclamo al Garante e non è soddisfatto dell'esito ovvero se il reclamo non ha avuto successo, può ancora rivolgersi al giudice ordinario (nel termine di 30 giorni dalla comunicazione del provvedimento) al fine di tutelare i propri diritti e, come vedremo, richiedere -in aggiunta- il risarcimento del danno. Per garantire che l'interessato e i titolari/responsabili abbiano sempre la possibilità di portare il proprio caso davanti a un tribunale, indipendentemente dalla via inizialmente scelta, è previsto in ogni caso che entrambe le parti possano sempre ricorrere in via giurisdizionale contro le decisioni del Garante.

La tutela giurisdizionale

È previsto infine il ricorso all'autorità giudiziaria[112] per il quale il legislatore europeo, con riguardo al luogo, ovvero allo Stato membro cui far riferimento, ha

[110] GDPR art. 4 - Definizioni, che al punto 12 afferma "*violazione dei dati personali: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati.*"
[111] DATA BREACH https://www.garanteprivacy.it/data-breach
[112] Decreto Legislativo 30 giugno 2003, n. 196 recante il "*Codice in materia di protezione dei dati personali*" Titolo I - Tutela amministrativa e giurisdizionale, Capo 0.I Alternatività delle forme di tutela, art. 140-bis - Forme alternative di tutela.

definito due criteri alternativi[113], infatti le azioni legali contro il titolare/responsabile del trattamento possono essere promosse:

1) dinnanzi all'autorità giurisdizionale dello Stato membro in cui il titolare o il responsabile del trattamento hanno uno stabilimento/sede;
2) dinnanzi all'autorità giurisdizionale dello Stato membro in cui l'interessato risiede abitualmente.

L'intenzione del legislatore è chiaramente quella di agevolare l'interessato e lasciarlo libero di scegliere la giurisdizione di competenza a lui più comoda. Tuttavia, vi è un'eccezione a questa regola, che si applica quando il titolare o il responsabile del trattamento dei dati è un'autorità pubblica, agente nell'esercizio dei pubblici poteri in uno Stato membro; in tale circostanza, ha giurisdizione il giudice dello Stato dell'autorità pubblica in questione. In Italia, la competenza in materia di azioni legali per il risarcimento del danno spetta generalmente al giudice ordinario al quale l'interessato ha la possibilità di chiedere misure inibitorie, proprio come con il reclamo al Garante, ma c'è un elemento aggiuntivo fondamentale: la possibilità di richiedere il risarcimento del danno ingiusto subito. Questa opzione consente all'interessato di ottenere un risarcimento economico per qualsiasi danno subito a causa della violazione dei propri diritti relativi alla protezione dei dati personali. Solo il tribunale può condannare il titolare del trattamento illecito al risarcimento dei danni occorsi all'interessato; è quindi evidente che il ricorso all'autorità giudiziaria offre una tutela più ampia e include la possibilità di ottenere un ristoro economico per il danno subito.

[113] GDPR art. 79 - Diritto a un ricorso giurisdizionale effettivo nei confronti del titolare del trattamento o del responsabile del trattamento, che al comma 2 afferma: "*Le azioni nei confronti del titolare del trattamento o del responsabile del trattamento sono promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui il titolare del trattamento o il responsabile del trattamento ha uno stabilimento. In alternativa, tali azioni possono essere promosse dinanzi alle autorità giurisdizionali dello Stato membro in cui l'interessato risiede abitualmente, salvo che il titolare del trattamento o il responsabile del trattamento sia un'autorità pubblica di uno Stato membro nell'esercizio dei pubblici poteri.*"

Nel contesto in analisi, come vedremo più in dettaglio nel paragrafo successivo, è fondamentale far notare sin da ora che il danno non può essere semplicemente l'evento dannoso in sé, ossia l'illecito trattamento dei dati, ma piuttosto, è necessario che si verifichi un pregiudizio effettivo alla sfera di interessi del danneggiato. Si noti che, secondo le comuni regole dovrebbe essere il danneggiato a darne prova, ricorrendo eventualmente a presunzioni e fatti noti e dimostrando i seguenti elementi:

1. la violazione delle norme di trattamento dei dati (trattamento illecito);
2. la gravità del pregiudizio subito, che è rilevante per quantificare l'entità del risarcimento;
3. il nesso di causalità tra il trattamento dei dati e l'evento dannoso.

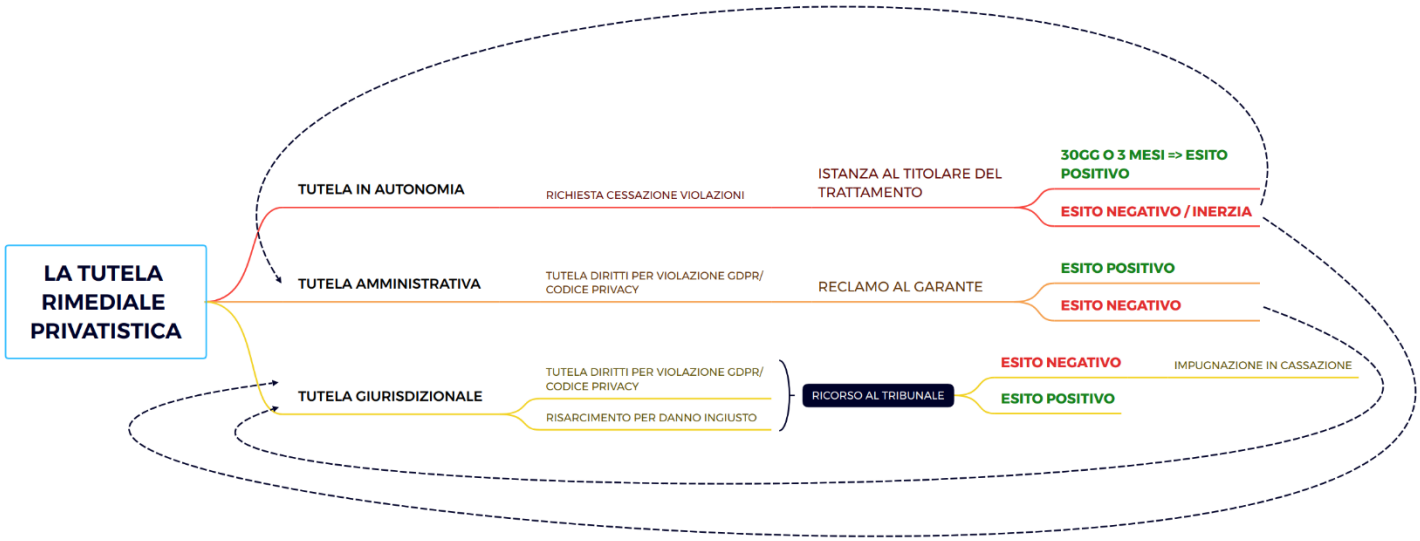
Tuttavia, l'interessato può anche limitarsi a segnalare la sola violazione dei principi e delle regole del GDPR, mentre sarà il titolare del trattamento, in conformità al principio di responsabilizzazione, a dover provare di aver agito in conformità al GDPR. Per evitare la responsabilità, egli deve dunque fornire una prova positiva e dimostrare che ha valutato correttamente il rischio dell'attività, a condizione che il rischio sia prevedibile,[114] e abbia attuato le misure organizzative e di sicurezza necessarie per eliminare o ridurre il rischio associato all'attività. Infine, va notato che il provvedimento che decide il ricorso può essere impugnato solo davanti alla Corte di cassazione.

Si badi che la tutela davanti al Garante e quella davanti al giudice sono alternative, il che significa che l'interessato deve sceglierne una e non può utilizzarle entrambe contemporaneamente per la stessa violazione dei diritti. Tuttavia, sia il reclamo al Garante che il ricorso al giudice sono stati predisposti dal Legislatore per agevolare l'azione dell'interessato e in ogni caso per far sì che il Garante compia la sua funzione di "guardiano" in tema di protezione dei dati personali.

[114] Come si vedrà più avanti con riguardo al danno, escludendo dunque il caso fortuito o di forza maggiore.

Infine, come accennato e anche se non oggetto del presente elaborato, è bene osservare che, oltre ai rimedi civilistici, il GDPR prevede sanzioni amministrative e penali, che rappresentano uno strumento assai efficace per affrontare i rischi derivanti dal trattamento su larga scala dei dati personali, poiché tali rischi interessano principalmente la collettività e possono sfuggire ai singoli interessati.

Mappa concettuale 8 – La tutela rimediale privatistica



Il Profilo soggettivo

La legittimazione attiva

Il GDPR esclude esplicitamente dall'ambito della sua applicazione i trattamenti di dati personali effettuati per scopi strettamente personali o familiari.[115] Ciò premesso, il GDPR stabilisce una vasta legittimazione attiva per richiedere il risarcimento dei danni causati dalla violazione delle norme sulla protezione dei dati personali. Come si vedrà, l'interessato è la figura principale in questo contesto, ma anche i terzi che subiscono danni (diretti o indiretti) collegati all'uso improprio di dati personali possono avere diritto al risarcimento. L'art. 82 del GDPR, infatti, è fondamentale per determinare la responsabilità e il risarcimento dei danni derivanti da violazioni del Regolamento, ed afferma che:

> "*Chiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

L'uso da parte del Legislatore del termine "*chiunque*" rende ben chiaro che la possibilità di chiedere un risarcimento per danno ingiusto spetta ad una pluralità di soggetti; principio che -peraltro- riflette una continuità con la Direttiva precedente e segue la stessa logica del codice della privacy iniziale, il quale affermava similmente il dovere di risarcire il danno causato "*ad altri*".
Pur restando chiaro che l'interessato è il soggetto principale legittimato ad agire in tali casi, poiché il Regolamento è principalmente rivolto alle persone fisiche, è

[115] GDPR - Considerando n. 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.*"

importante esaminare in che termini anche altri soggetti oltre all'interessato abbiano il diritto di richiedere il risarcimento ai sensi dell'art. 82 del GDPR.
Una prima categoria di terzi diversi dall'interessato che potrebbero patire dei danni, sono i portatori di interessi familiari meritevoli di tutela. Indipendentemente dalla natura specifica di tali interessi familiari, è necessario che il terzo abbia subito una lesione di un interesse proprio. Questo interesse potrebbe derivare dal fatto che il soggetto terzo appartiene, ad esempio, al nucleo familiare dell'interessato deceduto. In particolare, un parente stretto potrebbe avere diritto al risarcimento se il suo onore viene leso a causa della divulgazione di dati personali dell'interessato in virtù del loro legame familiare. Con riguardo al caso in cui l'interessato è deceduto, la possibilità di richiedere il risarcimento dipende dal momento in cui si è verificato l'evento dannoso, ovvero se è avvenuto prima o dopo la morte dell'interessato. Nel primo scenario, gli eredi saranno legittimati a richiedere il risarcimento per i danni subiti dal defunto; nel secondo, la legittimazione consente a soggetti diversi dall'interessato di esercitare i diritti relativi ai dati personali di persone decedute, anche se va precisato che chi agisce come mandatario dell'interessato deceduto non potrà ottenere il risarcimento che sarebbe spettato a quest'ultimo se fosse ancora in vita.[116]

[116] THOBANI S., art. 82 - Diritto al risarcimento e responsabilità, in BARBA A. E PAGLIANTINI S., Commentario del Codice civile delle persone, leggi correlate Vol. II, UTET giuridica, Roma, 2019, P. 1263-1267

La legittimazione passiva e le nuove figure tipiche

Per quanto riguarda i soggetti passivi, coloro che possono essere ritenuti responsabili per il risarcimento dei danni in caso di trattamento illecito sono le seguenti figure:

1) il titolare del trattamento;
2) i co-titolari del trattamento;
3) il responsabile del trattamento;
4) i sub-responsabili;
5) i co-responsabili del trattamento.

Si vedrà di seguito come il regime giuridico applicabile varia in base alla qualificazione soggettiva.

Il titolare del trattamento è responsabile per il danno derivante da un trattamento che viola il GDPR. Questo vale anche per i co-titolari del trattamento, e se ci sono più co-titolari coinvolti nello stesso trattamento essi risponderanno in solido. Per quanto riguarda il responsabile del trattamento e i co-responsabili, ci sono condizioni applicative diverse. I sub-responsabili non rispondono direttamente nei confronti dell'interessato ai sensi del GDPR, ma potranno essere chiamati a rispondere in sede di rivalsa da parte del responsabile del trattamento. Quando sono coinvolti più titolari o più responsabili nello stesso trattamento, vi è un'obbligazione risarcitoria solidale per il danno subito dall'interessato. Ciò significa che ognuno dei soggetti è responsabile per l'intero ammontare del danno, garantendo così il pieno risarcimento all'interessato. Va tuttavia specificato che, internamente, si può valutare il contributo causale individuale nella determinazione della responsabilità di ciascun soggetto nella catena di trattamento dei dati. Infatti, i delegati del titolare, i procuratori speciali e gli incaricati, pur essendo figure non previste dal GDPR, sono tutti responsabili in base al loro effettivo contributo alla causazione del danno nei rapporti interni con il titolare o con il responsabile del trattamento

in base a quanto stabilito dall'art. 2043 del Codice civile[117]. Inoltre, il principio dell'azione di regresso consente a un titolare o responsabile del trattamento che ha pagato l'intero risarcimento del danno, di proporre successivamente un'azione di regresso contro gli altri titolari o responsabili coinvolti nello stesso trattamento, per la parte di risarcimento corrispondente alla loro responsabilità per il danno.

Tali norme riflettono la volontà del Legislatore europeo di accrescere la tutela dell'interessato danneggiato, prendendo in considerazione le circostanze specifiche dell'attività di trattamento dei dati, l'organizzazione ad essa collegata e il livello di diligenza adottato da ciascun soggetto coinvolto nel trattamento.

Al riguardo, all'art. 82.4, il GDPR dispone che:

> "*Qualora più titolari del trattamento o responsabili del trattamento oppure entrambi il titolare del trattamento e il responsabile del trattamento siano coinvolti nello stesso trattamento e siano, ai sensi dei paragrafi 2 e 3, responsabili dell'eventuale danno causato dal trattamento, ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.*"

Tutto ciò mira a fornire una protezione efficace dei diritti e delle libertà dell'interessato danneggiato a causa del trattamento dei dati personali, soprattutto quando vi sono molti soggetti coinvolti in questa attività, a garanzia del "*pieno ed effettivo risarcimento dell'interessato che ha subito il danno.*"[118]

[117] Codice civile art. 2043 - Risarcimento per fatto illecito: "*Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno.*"

[118] GDPR - Considerando n. 146

Il titolare del trattamento

Il Titolare del Trattamento (Controller)[119] è

> "*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*".

In altre parole, si tratta del soggetto che, in autonomia o in collaborazione con altri, decide scopi e metodi del trattamento dei dati personali. Piu specificatamente, con riguardo alle responsabilità, considerando la natura, l'ambito di applicazione, il contesto e gli obiettivi del trattamento, nonché i diversi rischi per i diritti e le libertà delle persone fisiche, il titolare del trattamento deve adottare (e dimostrare) l'implementazione di misure tecniche e organizzative adeguate atte a garantire che il trattamento sia conforme al Regolamento. Queste misure devono essere riviste e aggiornate quando necessario[120]. Inoltre, l'adesione a codici di condotta, incoraggiati dal Legislatore al fine di contribuire alla corretta applicazione del GDPR[121], sebbene non costituisca una liberatoria automatica, potrà essere utilizzata come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento e, di conseguenza, per mitigare la responsabilità in caso di azione di risarcimento danni per trattamento illecito dei dati personali.

[119] GDPR art. 4, punto 7 - Definizioni
[120] GDPR art. 24 - Responsabilità del titolare del trattamento
[121] GDPR art. 40 - Codici di condotta

I contitolari del trattamento

Nel contesto di un processo di trattamento dei dati personali di particolare complessità, è ammessa la situazione in cui più titolari del trattamento collaborino congiuntamente per determinare gli scopi e i metodi del trattamento. Questa situazione è definita come "*contitolarità del trattamento*"[122]. L'elemento chiave in questo scenario è la determinazione congiunta delle finalità e delle modalità del trattamento, che ha implicazioni anche sul piano della responsabilità congiunta per eventuali fatti illeciti. I contitolari devono stabilire in modo trasparente le rispettive responsabilità attraverso un accordo interno (naturalmente in forma scritta, anche in formato elettronico)[123], che contenga anche disposizioni sul rispetto degli obblighi imposti dal Regolamento, compreso il trattamento dei dati dell'interessato e le relative comunicazioni.[124]

Laddove invece vi sia un accordo interno, esso può anche designare un punto di contatto per l'interessato e deve essere messo a disposizione dello stesso.

È bene evidenziare che, in ogni caso, indipendentemente da quanto stabilito nell'accordo interno, l'interessato può esercitare a sua discrezione i propri diritti e chiedere il risarcimento del danno nei confronti di ciascun titolare del trattamento, rispondendo essi in solido, come ben chiarito dal GDPR all'art. 82.4:

> "*…ogni titolare del trattamento o responsabile del trattamento è responsabile in solido per l'intero ammontare del danno, al fine di garantire il risarcimento effettivo dell'interessato.*"

[122] GDPR art. 26 - Contitolari del trattamento

[123] È prevista la forma scritta al fine di definire con chiarezza e trasparenza ruoli, mansioni e responsabilità inerenti all'osservanza degli obblighi previsti, in particolare per quanto concerne la tutela dei diritti dell'interessato.

[124] GDPR art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato; art. 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato.

Il responsabile del trattamento, la sub-responsabilità e co-responsabilità

Il responsabile del trattamento (Processor)[125] è:

> "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento*".

Il titolare del trattamento può designare il responsabile del trattamento, che assume la responsabilità di garantire, per quanto di sua competenza, che il trattamento dei dati sia conforme al GDPR e che vengano adottate misure tecniche e organizzative adeguate al fine di proteggere i diritti dell'interessato.
Il responsabile del trattamento dei dati personali ha a sua volta facoltà di designare un altro soggetto, ovvero il sub-responsabile del Trattamento, al fine di svolgere specifiche attività di trattamento. Tuttavia, non può farlo senza prima ottenere un'autorizzazione scritta dal titolare del trattamento e se questa designazione avviene senza rispettare l'obbligo di informare e ottenere il consenso dal titolare del trattamento, è invalida. In tal caso, la responsabilità rimane esclusivamente del responsabile del trattamento. Se il titolare del trattamento concede un'autorizzazione scritta generale, il responsabile del trattamento deve informare il titolare del trattamento di qualsiasi futura modifica riguardante l'aggiunta o la sostituzione di altri responsabili del trattamento. Questo dà al titolare del trattamento l'opportunità di opporsi a tali modifiche se lo desidera. Tutti i trattamenti dei dati personali da parte del responsabile del trattamento devono essere regolamentati da un negozio giuridico conforme al diritto dell'Unione o degli Stati membri, che deve essere redatto in forma scritta o in una forma elettronica equivalente e deve specificare vari dettagli, tra cui le istruzioni documentate del titolare del trattamento, le misure di sicurezza, i diritti delle persone cui appartengono i dati e tutti gli altri obblighi in capo al responsabile.

[125] GDPR art. 4, punto 8 - Definizioni, art. 28 - Responsabile del trattamento

La co-responsabilità invece si verifica quando più responsabili del trattamento lavorano insieme per gestire gli stessi dati personali per gli stessi scopi. In queste specifiche situazioni, i responsabili del trattamento condividono le responsabilità e devono collaborare per garantire la conformità al GDPR e, anche in questo caso, è fondamentale stabilire chiaramente i rispettivi ruoli ed obblighi attraverso accordi scritti per evitare ambiguità e garantire l'attuazione di misure di sicurezza adeguate.

Con riguardo in particolare ai propri obblighi, il responsabile del trattamento, in base a quanto stabilito dall'art. 28 del GDPR[126], deve:

- trattare i dati personali solo in base a istruzioni documentate del titolare;
- garantire la riservatezza dei dati personali;
- implementare misure di sicurezza adeguate (come previsto dall'articolo 32 del GDPR[127]);
- rispettare le condizioni per coinvolgere altri responsabili;
- assistere il titolare nell'esercizio dei diritti degli interessati;
- assistere il titolare nel rispetto degli obblighi previsti dal GDPR in tema di
    - notifica di una violazione al Garante;[128]
    - comunicazione di una violazione all'interessato;[129]
    - valutazione d'impatto sulla protezione dei dati;[130]
    - consultazione preventiva dell'Autorità in caso di rischio elevato in assenza di misure;[131]
- cancellare o restituire i dati personali al termine del servizio, a meno che la legge richieda la conservazione;
- fornire al titolare le informazioni necessarie per dimostrare la conformità alle norme del GDPR e collaborare alle attività di revisione.

[126] GDPR art. 28 - Responsabile del trattamento
[127] GDPR art. 32 - Sicurezza del trattamento
[128] GDPR art. 33 - Notifica di una violazione dei dati personali all'autorità di controllo
[129] GDPR art. 34 - Comunicazione di una violazione dei dati personali all'interessato
[130] GDPR art. 35 - Valutazione d'impatto sulla protezione dei dati
[131] GDPR art. 36 - Consultazione preventiva

Il responsabile, come già accennato[132], ha inoltre l'onere della tenuta del registro dei trattamenti ove andrà indicato quanto segue:

- le finalità del trattamento;
- la descrizione delle categorie di interessati e di dati personali;
- le categorie di destinatari a cui i dati sono stati o saranno comunicati;
- gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- i termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- la descrizione generale delle misure di sicurezza adottate.

Egli, inoltre, è tenuto ad informare il titolare se ritiene che un'istruzione violi il GDPR o, più in generale, se ritiene che vi sia una violazione di una qualsivoglia normativa relativa alla protezione dei dati.
Il responsabile del trattamento dei dati personali, quindi, è chiaramente soggetto a responsabilità giuridiche ben precise in caso di violazione delle normative previste dal GDPR e tali circostanze possono dar luogo all'obbligo di risarcimento dei danni. In primo luogo, se il titolare del trattamento fornisce al responsabile istruzioni documentate in merito al trattamento dei dati personali e il responsabile non segue tali istruzioni o apporta modifiche non autorizzate, provocando un danno all'interessato o a terzi, il responsabile potrebbe essere coinvolto. Inoltre, il Regolamento impone disposizioni chiare e dettagliate in merito alla protezione dei dati personali e se il responsabile del trattamento non rispetta queste disposizioni e questa violazione dei principi fondamentali del GDPR comporta un danno per l'interessato o terzi, il responsabile può essere coinvolto. Ed ancora, quando il titolare del trattamento e il responsabile stipulano un contratto o un altro atto giuridico per disciplinare il trattamento dei dati personali, il responsabile è legalmente obbligato a rispettare scrupolosamente le

[132] Si veda: Capitolo Terzo - L'accountability, L'accountability nel GDPR

clausole di tale contratto; l'inosservanza di tali clausole contrattuali, se causa un danno, può comportare responsabilità.

Il tema della sicurezza dei dati è molto sentito ed è un requisito fondamentale nel contesto della protezione della privacy; di conseguenza il GDPR richiede che il responsabile del trattamento studi, pianifichi e metta in atto adeguate misure tecniche e organizzative per garantire la sicurezza dei dati personali, eventualmente anche avvalendosi a sua volta di figure esterne esperte[133]. Se il responsabile non adotta queste misure o non le implementa in modo appropriato, causando una violazione della sicurezza dei dati e un danno all'interessato, potrebbe essere ritenuto responsabile.

Al termine dei servizi di trattamento dei dati, il responsabile è tenuto a cancellare o restituire i dati personali in conformità con le disposizioni del GDPR e con le istruzioni del titolare. La mancata esecuzione di questi adempimenti, se causa un danno all'interessato o al titolare, può comportare responsabilità.

Ed infine, il responsabile è obbligato a informare tempestivamente il titolare del trattamento se identifica una violazione dei dati; la mancata segnalazione tempestiva della violazione che provoca un danno all'interessato, può comportare responsabilità.

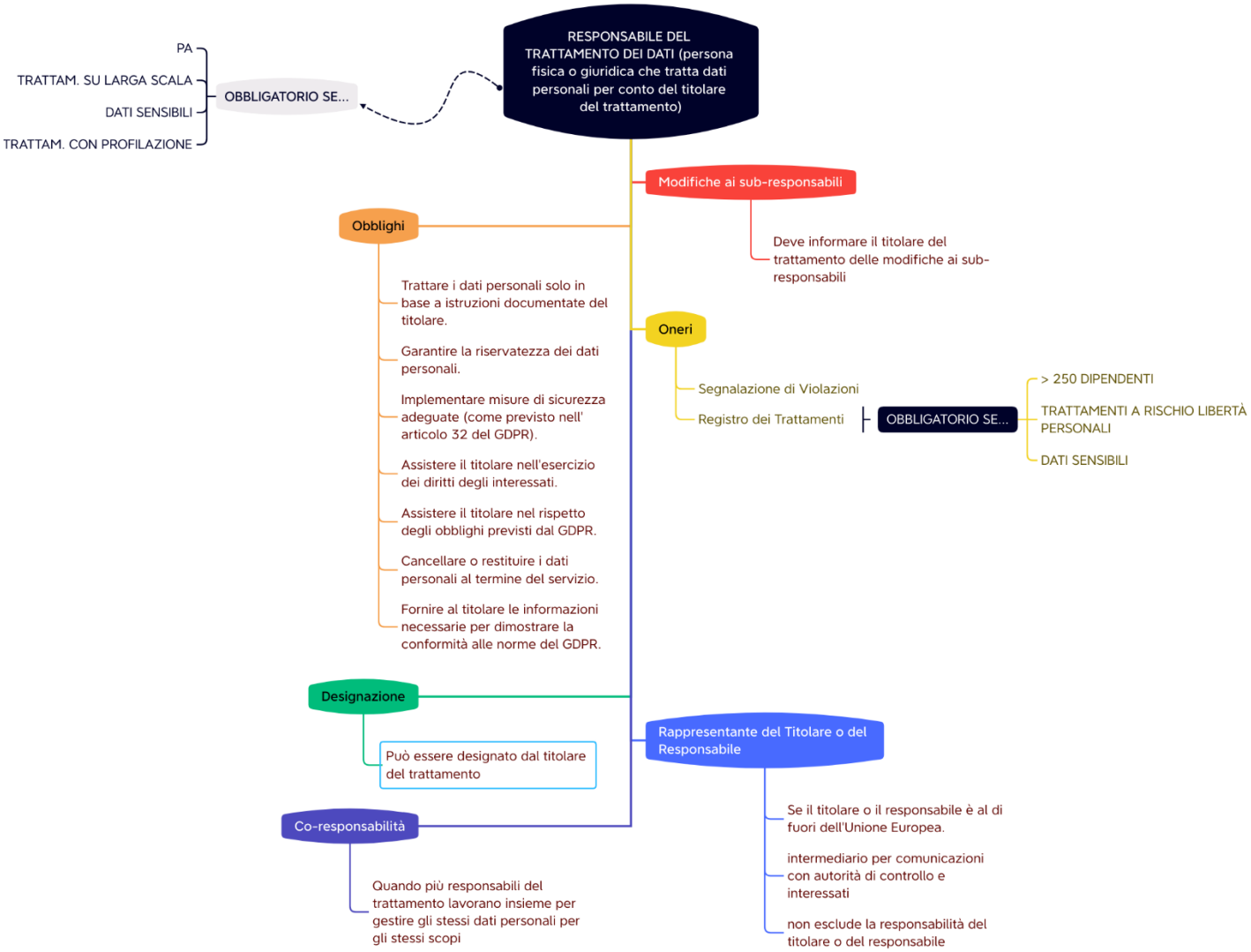
Va sottolineato che il responsabile del trattamento non risponde per le violazioni del GDPR commesse dal titolare del trattamento, ma piuttosto per le proprie azioni od omissioni che provocano un danno derivante dalla inosservanza delle norme del GDPR o dei contratti tra le parti. Le sanzioni e le responsabilità sono determinate dalla Autorità preposte[134] in base alla gravità della violazione e alle circostanze specifiche che saranno valutate caso per caso.

---

[133] Si pensi, ad esempio, al coinvolgimento di Società specializzate operanti nel settore dell'ICT ovvero di consulenti informatici esperti in sicurezza informatica per il mascheramento o il criptaggio delle informazioni, di esperti di strumenti hardware e software adibiti alla trasmissione dei dati o alla conservazione dei dati, al backup di archivi elettronici o esperti di sistemi informatici antintrusione come firewall, antivirus, ecc.

[134] Si veda: Capitolo quarto - La responsabilità civile da illecito trattamento dei dati personali, La tutela rimediale.

Mappa concettuale 9 - Il Responsabile del trattamento



Il rappresentante del titolare o del responsabile

Il GDPR prevede che, nel caso in cui il titolare del trattamento o il responsabile del trattamento siano stabiliti al di fuori dell'Unione Europea, essi debbano nominare per iscritto un rappresentante (representative)[135] nell'Unione Europea[136]. Questo rappresentante ha il compito di agire come intermediario, agendo in aggiunta o in sostituzione del titolare del trattamento o del responsabile del trattamento, specialmente per quanto riguarda le comunicazioni con le autorità di controllo per tutte le questioni relative al trattamento dei dati. Va notato che la designazione di un rappresentante da parte del titolare del trattamento o del responsabile del trattamento non esclude responsabilità di questi ultimi per qualsiasi trattamento illecito dei dati personali. In altre parole, il titolare del trattamento o il responsabile del trattamento rimangono soggetti a possibili azioni legali, comprese azioni di risarcimento danni, che potrebbero essere intraprese contro di loro, nonostante l'esistenza del rappresentante che -di fatto- non è responsabile per i danni derivanti dal trattamento illecito dei dati personali.

Il Responsabile della protezione dei dati – DPO (Data Protection Officer)

Come già accennato in precedenza, il DPO[137] è una figura nuova, dotata di competenze specializzate[138], autonomia decisionale, imparzialità ed indipendenza, la cui nomina non è solitamente obbligatoria. Deve essere un

[135] GDPR art. 4, punto 17 - Definizioni
[136] GDPR art. 27 - Rappresentanti di titolari del trattamento o dei responsabili del trattamento non stabiliti nell'Unione, Considerando n. 80
[137] GDPR art. 4 - Definizioni, punto 8 e Sezione 4 - Responsabile della protezione dei dati
[138] Federprivacy, Certificazione DPO: i chiarimenti del Garante sulla Norma UNI: non è necessario, come ha chiarito il Garante, possedere titoli specifici o certificazioni per svolgere le funzioni previste dal GDPR. Tuttavia, le certificazioni volontarie possono comunque contribuire all'accountability. https://www.federprivacy.org/attivita/certificazione-dpo-i-chiarimenti-del-garante-sulla-norma-uni

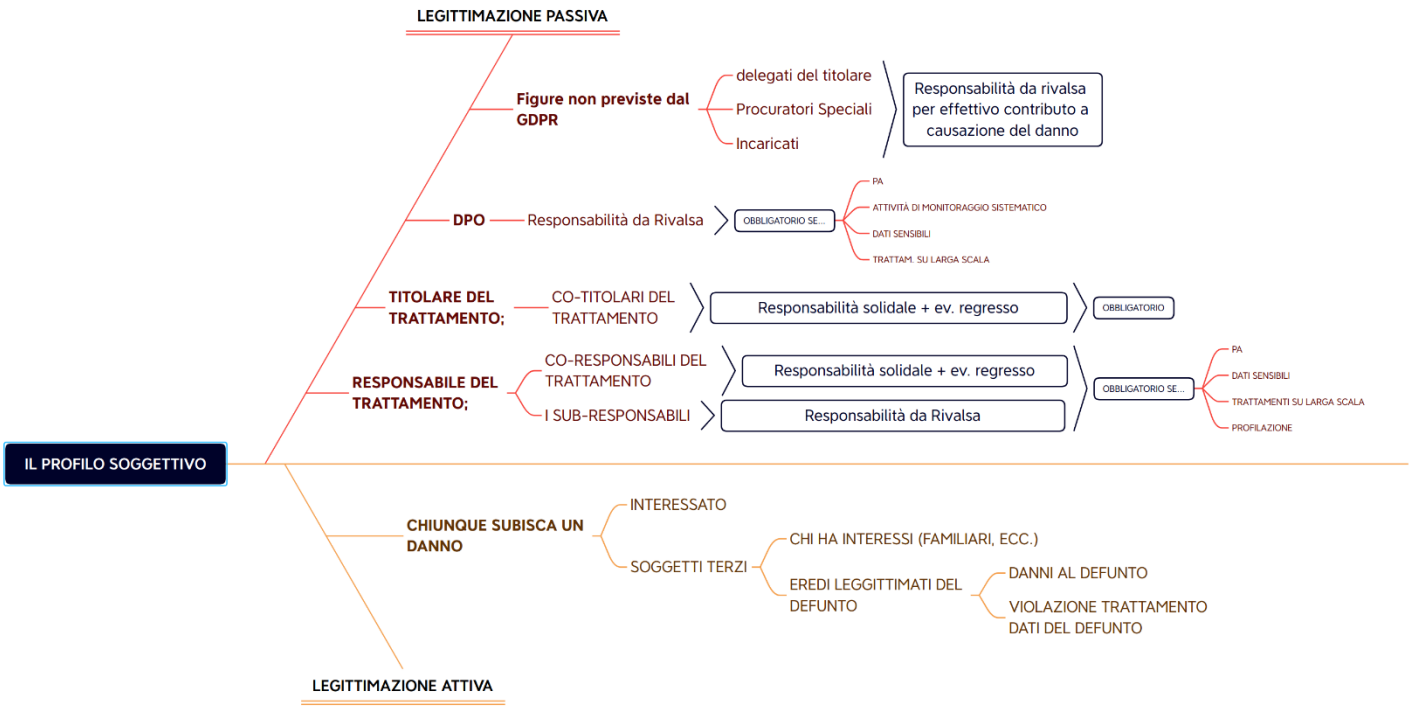
esperto nelle norme e procedure relative alla protezione dei dati personali, in grado di gestire le relazioni non solo con le persone coinvolte nel trattamento dei dati personali, ma anche con l'autorità garante. Egli può essere un dipendente del titolare o del responsabile del trattamento oppure può essere una figura esterna e svolgere il suo ruolo in base a un contratto di consulenza. Il DPO è dunque privo di conflitti di interesse, dotato di risorse adeguate (anche economiche) e una linea di reporting diretta all'apice dell'organizzazione del titolare del trattamento o del responsabile del trattamento che lo ha nominato. Nell'adempimento dei suoi compiti, il DPO ha la responsabilità di tenere adeguatamente conto dei rischi connessi al trattamento dei dati, considerando la natura, l'ambito di applicazione, il contesto e le finalità di tali trattamenti. Tale figura è responsabile di aspetti tecnici, normativi e procedurali, in particolare di:

1) assegnare responsabilità, sensibilizzare e fornire formazione al personale coinvolto nei trattamenti e nelle attività di controllo correlate;
2) offrire consulenza sulla valutazione d'impatto sulla protezione dei dati, se richiesta, e supervisionare il suo processo[139];
3) collaborare con l'autorità garante;
4) agire come punto di contatto per l'autorità garante per questioni legate al trattamento dei dati, inclusa la consultazione preventiva.[140]

Con riguardo alla responsabilità civile, va precisato che il DPO non ha responsabilità all'esterno[141], ovvero a fronte di richieste di risarcimento mosse dall'interessato. Tuttavia, sia il titolare che il responsabile che lo hanno designato, avranno facoltà di rivalersi "internamente" qualora l'azione esterna di risarcimento del danno nei loro confronti avrà visto l'accoglimento del Giudice per negligenze nella gestione del processo o nell'applicazione delle norme previste da parte del DPO.

[139] GDPR art. 35 - Valutazione d'impatto sulla protezione dei dati
[140] GDPR art. 36 - Consultazione preventiva
[141] TOSI E., Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale, Milano, 2019, P. 91

Mappa concettuale 10 - Il profilo soggettivo



Il Profilo oggettivo

I principi fondamentali del trattamento dei dati personali

All'articolo 5[142] il GDPR indica le principali condizioni che devono essere rispettate per garantire la legittimità del trattamento dei dati, in continuità con quanto stabilito dalle precedenti norme[143]. L'articolo 5 del GDPR svolge un ruolo importante, anticipando le disposizioni dettagliate presenti negli articoli successivi e introducendo i principi generali di liceità[144], correttezza e trasparenza[145] che rappresentano le fondamenta per le norme specifiche sulla gestione dei dati personali stabilite dal Legislatore europeo. L'articolo 5, infatti, contribuisce a delineare le caratteristiche fondamentali del trattamento dei dati

[142] GDPR art. 5 - Principi applicabili al trattamento di dati personali

[143] Si veda: Capitolo Primo - Premessa, Il contesto normativo generale di riferimento.

[144] GDPR - Considerando n. 39: "*Qualsiasi trattamento di dati personali dovrebbe essere lecito e corretto. Dovrebbero 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. 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 alle persone fisiche interessate e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che le riguardano. È opportuno che le persone fisiche siano sensibilizzate ai rischi, alle norme, alle garanzie e ai diritti relativi al trattamento dei dati personali, nonché alle modalità di esercizio dei loro diritti relativi a tale trattamento. In particolare, le finalità specifiche del trattamento dei dati personali dovrebbero essere esplicite e legittime e precisate al momento della raccolta di detti dati personali. I dati personali dovrebbero essere adeguati, pertinenti e limitati a quanto necessario per le finalità del loro trattamento. Da qui l'obbligo, in particolare, di assicurare che il periodo di conservazione dei dati personali sia limitato al minimo necessario. I dati personali dovrebbero essere trattati solo se la finalità del trattamento non è ragionevolmente conseguibile con altri mezzi. Onde assicurare che i dati personali non siano conservati più a lungo del necessario, il titolare del trattamento dovrebbe stabilire un termine per la cancellazione o per la verifica periodica. È opportuno adottare tutte le misure ragionevoli affinché i dati personali inesatti siano rettificati o cancellati. 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.*"

[145] GDPR art. 12 - Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato

personali, mirando a regolare il comportamento delle organizzazioni che trattano dati personali affinché i trattamenti non ledano i diversi interessi in gioco[146]. Esso stabilisce gli elementi fondamentali applicabili al trattamento e, più in dettaglio, disciplina che i dati personali siano:

> *"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 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*

[146] ACHILLE D., art. 5 - Principi applicabili al trattamento di dati personali, in BARBA A. E PAGLIANTINI S., Commentario del Codice civile delle persone, leggi correlate Vol. II, UTET giuridica, Roma, 2019, P. 127-140

adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)."

Inoltre, al punto 2 dell'art. 5 è stabilito che:

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

Il principio di liceità, ripreso poi dall'art. 6, è fondato sull'idea che qualsiasi limitazione alla protezione dei dati personali deve essere chiaramente prevista dalla legge e deve servire a uno scopo legittimo e proporzionato. Questo principio svolge un ruolo chiave nel bilanciare i diritti alla protezione dei dati personali con altri interessi; la liceità non solo contribuisce a determinare le basi giuridiche per il trattamento dei dati, ma fornisce anche un quadro generale per valutare la legittimità di tale trattamento, considerando i requisiti specifici stabiliti dalla legge.

Il principio di correttezza, strettamente legato alla liceità, riguarda il modo in cui i dati personali devono essere trattati, si basa su principi di buona fede e richiede che il titolare del trattamento metta in atto tutti gli atti necessari a proteggere l'interessato, sempre nel rispetto del principio di proporzionalità.

Entrambi i principi di liceità e correttezza sono cruciali per garantire una corretta gestione dei dati personali e contribuiscono alla tutela dell'autodeterminazione informativa dell'individuo.

Il principio di trasparenza, prevede che le modalità di raccolta, uso e consultazione dei dati personali siano chiare per le persone fisiche interessate, elemento questo fondamentale per consentire alle persone di esercitare i propri diritti, inclusa la revoca del consenso. La chiarezza e l'accessibilità delle informazioni relative al trattamento, incluse le finalità e l'identità del titolare del trattamento, sono elementi essenziali di questo principio.

Il principio della limitazione della finalità, sancito anch'esso dall'art. 5 del GDPR, sottolinea l'importanza di trattare i dati personali esclusivamente per scopi specifici e legittimi, con una chiara determinazione di tali finalità. Questo principio offre una garanzia agli individui in quanto definisce i limiti del trattamento dei loro dati e protegge i loro diritti. L'esattezza dei dati è un aspetto

fondamentale, e il principio dell'esattezza richiede che i dati siano accurati e aggiornati. È responsabilità del titolare del trattamento adottare misure adeguate al fine di correggere o eliminare dati inesatti in relazione alle finalità del trattamento. Questo principio è strettamente collegato agli articoli contenuti nella "Sezione 3 - Rettifica e cancellazione"[147], che consentono agli interessati di richiedere la correzione o la cancellazione di dati inesatti o incompleti. Il principio della stretta finalità enfatizza che i dati personali devono essere raccolti e trattati solo per scopi specifici e legittimi, garantendo che tali finalità siano esplicite. Un aspetto saliente di questo principio riguarda la compatibilità del trattamento per finalità ulteriori: il GDPR chiarisce che il trattamento per finalità ulteriori è consentito quando è finalizzato all'archiviazione nel pubblico interesse, alla ricerca scientifica, storica o a fini statistici. Ciò richiede una valutazione della compatibilità tra le finalità iniziali e quelle successive, considerando vari fattori come il contesto della raccolta dei dati e le aspettative dell'interessato.

Il principio di limitazione della conservazione stabilisce che i dati personali devono essere conservati solo per il tempo necessario per raggiungere le finalità del trattamento. Inoltre, i dati possono essere conservati per un periodo più lungo se trattati per archiviazione nel pubblico interesse, ricerca scientifica, storica o a fini statistici. Questo principio è strettamente legato al già menzionato diritto all'oblio, che consente agli interessati di richiedere la cancellazione dei propri dati quando non sono più necessari.

Altro principio importante è quello della minimizzazione dei dati, collegato ai principi di necessità, pertinenza, completezza e non eccedenza, che sottolineano l'importanza di raccogliere e trattare solo i dati che sono realmente necessari per scopi specifici e legittimi, a garanzia che il trattamento dei dati sia proporzionato alla finalità perseguita, ossia al minimo necessario per il loro scopo, riducendo al minimo il rischio di eccessiva raccolta o trattamento di dati personali. Questo principio si articola in due aspetti principali:

[147] GDPR art. 16 - Diritto di rettifica e artt. successivi

1. in primo luogo, la pertinenza implica che i dati personali oggetto di trattamento debbano essere direttamente collegati all'obiettivo del trattamento, il che significa che solo i dati strettamente necessari per il raggiungimento della finalità possono essere raccolti e trattati (ciò, a tutela dell'interessato, previene la raccolta e l'utilizzo di dati superflui o non pertinenti);
2. in secondo luogo, la limitazione richiede che il trattamento includa solo i dati essenziali per conseguire un preciso obiettivo specifico, ovvero che i dati non siano trattati se la finalità perseguita può essere raggiunta in modo ragionevole utilizzando mezzi diversi; ne consegue che il periodo di conservazione deve essere limitato al minimo necessario (il titolare/responsabile del trattamento deve stabilire termini per la cancellazione o per la revisione periodica per assicurare che i dati vengano conservati esclusivamente per il tempo strettamente necessario all'obiettivo specifico).

Il principio di integrità e riservatezza[148] rivela l'importanza di trattare i dati personali in modo da garantire la loro sicurezza[149] e protezione[150]. La sua applicazione richiede il costante impegno da parte del titolare/responsabile del trattamento per mettere in atto misure di sicurezza adeguate, siano esse di natura tecnica o organizzativa, in ogni caso commisurate alla tipologia di dati trattati e alle modalità di trattamento. La ragione dietro questa esigenza è quella di assicurare che i dati siano protetti in maniera proporzionata al rischio associato al loro trattamento. È importante notare che il GDPR ha elevato l'obbligo di garantire la sicurezza dei dati a un vero e proprio principio generale

[148] GDPR art. 5 - Principi applicabili al trattamento di dati personali, dove alla lettera "f" è stabilito che: "*dati personali sono: 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»)*."

[149] GDPR art. 32 - Sicurezza del trattamento

[150] GDPR art. 25 - Protezione dei dati fin dalla progettazione e protezione dei dati per impostazione predefinita

del trattamento dei dati personali. Questo significa che la sicurezza dei dati deve essere considerata in ogni fase del trattamento, dalla raccolta alla conservazione fino alla cancellazione. L'applicazione di questo principio richiede una valutazione attenta e continua dei rischi associati al trattamento dei dati. Inoltre, poiché il principio è formulato in modo generico, il titolare del trattamento ha il compito di individuare e attuare le misure di sicurezza appropriate in base alle circostanze specifiche per consentire di personalizzare le misure di sicurezza e soddisfare le esigenze individuali. Un obiettivo chiave di questo principio è prevenire accessi non autorizzati ai dati personali, garantendo che solo le persone autorizzate possano accedervi e dunque con un approccio mirato a prevenire la perdita o il danneggiamento accidentale dei dati.

Il GDPR all'articolo 6[151] stabilisce ulteriori criteri di legittimità del trattamento, con particolare riguardo al fine della correlata valutazione di illegittimità del comportamento[152]. Il trattamento è considerato legittimo solamente se si verifica almeno una delle seguenti condizioni:

> "*a) l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità;*
>
> *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;*

[151] GDPR art. 6 - Liceità del trattamento

[152] GDPR - Considerando n. 40: "*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*".

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. La lettera f) del primo comma non si applica al trattamento di dati effettuato dalle autorità pubbliche nell'esecuzione dei loro compiti."

Il principio della "*liceità*" del trattamento dei dati personali[153] è fondamentale per garantire una base giuridica solida e legittima per il trattamento dei dati personali e mira a trovare il delicato equilibrio tra la protezione dei diritti fondamentali dell'individuo e la promozione della libera circolazione delle informazioni nel mercato europeo, specialmente in un contesto in cui la raccolta di grandi quantità di dati (attraverso i già citati Big Data o IoT[154]) risulta essere un fenomeno assai rilevante ed in costante aumento.

Il GDPR stabilisce il divieto generale di trattamento dei dati personali, indicando che esso è consentito solo in determinate circostanze, ovvero laddove siano soddisfatte le "*condizioni di liceità*". Una di queste condizioni è la "*necessità*" di adempiere a un obbligo legale o l'esecuzione di un compito di interesse pubblico. Inoltre, il GDPR introduce una nuova condizione di liceità, ovvero il "*legittimo interesse*" del titolare del trattamento o di terze parti, a condizione che gli interessi o i diritti fondamentali della persona interessata non prevalgano. Questa condizione riconosce la possibilità di trattare dati personali senza richiedere il consenso, purché vi sia un legittimo interesse e non vi siano conseguenze negative per i diritti fondamentali dell'individuo.

[153] BOSA S., art. 6 - Liceità del trattamento, in BARBA A. E PAGLIANTINI S., Commentario del Codice civile delle persone, leggi correlate Vol. II, UTET giuridica, Roma, 2019, P. 141-154

[154] Si veda: Capitolo Secondo - La storia del diritto alla privacy, L'era dell'ICT.

È importante, inoltre, approfondire il concetto di consenso[155], che gioca un ruolo essenziale nel contesto del GDPR, che lo definisce come una manifestazione di volontà dell'individuo interessato che deve rispettare determinati requisiti, ovvero deve essere:

1) libera;
2) specifica;
3) informata;
4) inequivocabile.

Il consenso può essere espresso in vari modi, come una dichiarazione esplicita o un comportamento che indica l'assenso all'uso dei propri dati personali. Il GDPR stabilisce requisiti rigorosi per questo consenso, il che significa che una qualsiasi manifestazione di volontà non è sufficiente a rendere legittimo il trattamento dei dati personali: deve essere un consenso informato e volontario, e non deve essere soggetto a coercizione o indebito condizionamento. In altre parole, l'individuo deve essere opportunamente informato sull'uso previsto dei dati personali, compresi i diritti che gli spettano in relazione al trattamento dei dati; inoltre, il consenso non è valido se l'individuo è in una situazione di squilibrio o se l'operatore economico subordina l'offerta di un servizio o l'esecuzione di una prestazione al consenso dell'individuo. La *ratio legis* è quella di garantire che il consenso sia una scelta autodeterminata, consapevole e il più possibile scevra da influenze esterne.

Per garantire concretamente che l'individuo sia pienamente consapevole di come verranno utilizzati i suoi dati personali e dei diritti a sua disposizione, al titolare/

[155] GDPR art. 4 - Definizioni, che al punto 11 indica che: "*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*". Si vedano anche: art. 7 - Condizioni per il consenso; art. 8 - Condizioni applicabili al consenso dei minori in relazione ai servizi della società dell'informazione; art. 9 - Trattamento di categorie particolari di dati personali.

responsabile del trattamento sono imposti obblighi di informazione all'interessato[156].

Per rispettare i principi generali del trattamento, al titolare si impone di individuare e adottare adeguate misure tecniche ed organizzative considerando il livello tecnologico attuale[157], gli investimenti economici associati all'attuazione delle misure, nonché la natura, l'ambito di applicazione, il contesto e gli obiettivi del trattamento, insieme ai rischi per i diritti fondamentali e le libertà delle persone fisiche. Queste misure sono finalizzate a garantire il necessario livello di sicurezza in relazione al rischio di trattamento dei dati personali. Tali misure comprendono, ad esempio:

- il Data Masking, ossia la cifratura dei dati personali (pseudonimizzazione);
- la disponibilità in continuità dei sistemi ICT coinvolti nel trattamento attraverso, ad esempio, tecnologie software e/o hardware per il salvataggio ed il ripristino automatizzato dei dati (backup/restore) e tecnologie software e/o hardware antintrusione (firewall, antivirus, ecc.);
- sistemi ICT evoluti, in alta affidabilità e disaster recovery (per le organizzazioni più grandi o le Pubbliche Amministrazioni)[158], per il pronto ripristino della disponibilità delle funzionalità in caso di disastro (si pensi ad esempio ad un terremoto o ad una inondazione), di incidente fisico, tecnico o di intrusione;
- procedura per testare, valutare periodicamente l'efficacia delle misure tecniche e organizzative in atto.

Nel processo di valutazione dell'adeguatezza del livello di sicurezza, si presta particolare attenzione ai più significativi rischi derivanti dal trattamento, ovvero la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso accidentale o illegale ai dati personali trasmessi, conservati o altrimenti trattati.

---

[156] GDPR art. 13 - Informazioni da fornire qualora i dati personali siano raccolti presso l'interessato, art. 14 - Informazioni da fornire qualora i dati personali non siano stati ottenuti presso l'interessato

[157] Si veda: Capitolo secondo, l'era dell'ICT.

[158] AgID - Agenzia per l'Italia digitale, Linee guida per il disaster recovery delle pubbliche amministrazioni https://www.agid.gov.it/sites/default/files/repository_files/linee_guida/linee-guida-dr.pdf

È interessante notare che il GDPR mutua ancora il principio dell'accountability[159] attraverso -in questo caso- il richiamo all'efficacia mitigante dell'adesione ad uno dei numerosi codici di condotta[160], ovvero ad un meccanismo di certificazione[161]. Tali adesioni possono dimostrare la conformità ai requisiti previsti dall'articolo 32.1.[162] Inoltre, sia il titolare del trattamento che il responsabile del trattamento assicurano che chiunque agisca sotto la loro autorità e abbia accesso a dati personali, non tratti tali dati a meno che non sia stato istruito in merito dal titolare del trattamento, sempre che ciò non sia previsto dal diritto dell'Unione Europea o dagli Stati membri.

Nell'ambito di questa fase dell'analisi, è dunque importante sottolineare di nuovo l'importanza del principio di responsabilizzazione (accountability)[163], che, com'è ormai ben evidente, è presente nell'intero quadro regolatorio di tutto il GDPR. Questo principio comporta un passaggio significativo dalla responsabilità ex post a una responsabilizzazione ex ante, basata sulla prevenzione e la gestione dei rischi derivanti dal trattamento, senza imporre regole rigide e assolute. Lo stato dell'arte e la sostenibilità economica delle scelte effettuate dal titolare del trattamento per garantire l'adeguatezza delle misure tecniche e organizzative, in particolare per la protezione dei diritti fondamentali delle persone (come la riservatezza e la protezione dei dati personali e dell'identità personale), emergono in diverse parti del Regolamento. Le considerazioni e le scelte che gravano sul titolare/responsabile in merito ad una determinata situazione di un'organizzazione, assieme ai costi di attuazione, sono funzionali alla probabilità e alla gravità dei rischi specifici valutati responsabilmente[163]. Questi vincoli sono

[159] Si veda: Capitolo Terzo, L'accountability

[160] GDPR art. 40 - Codici di condotta

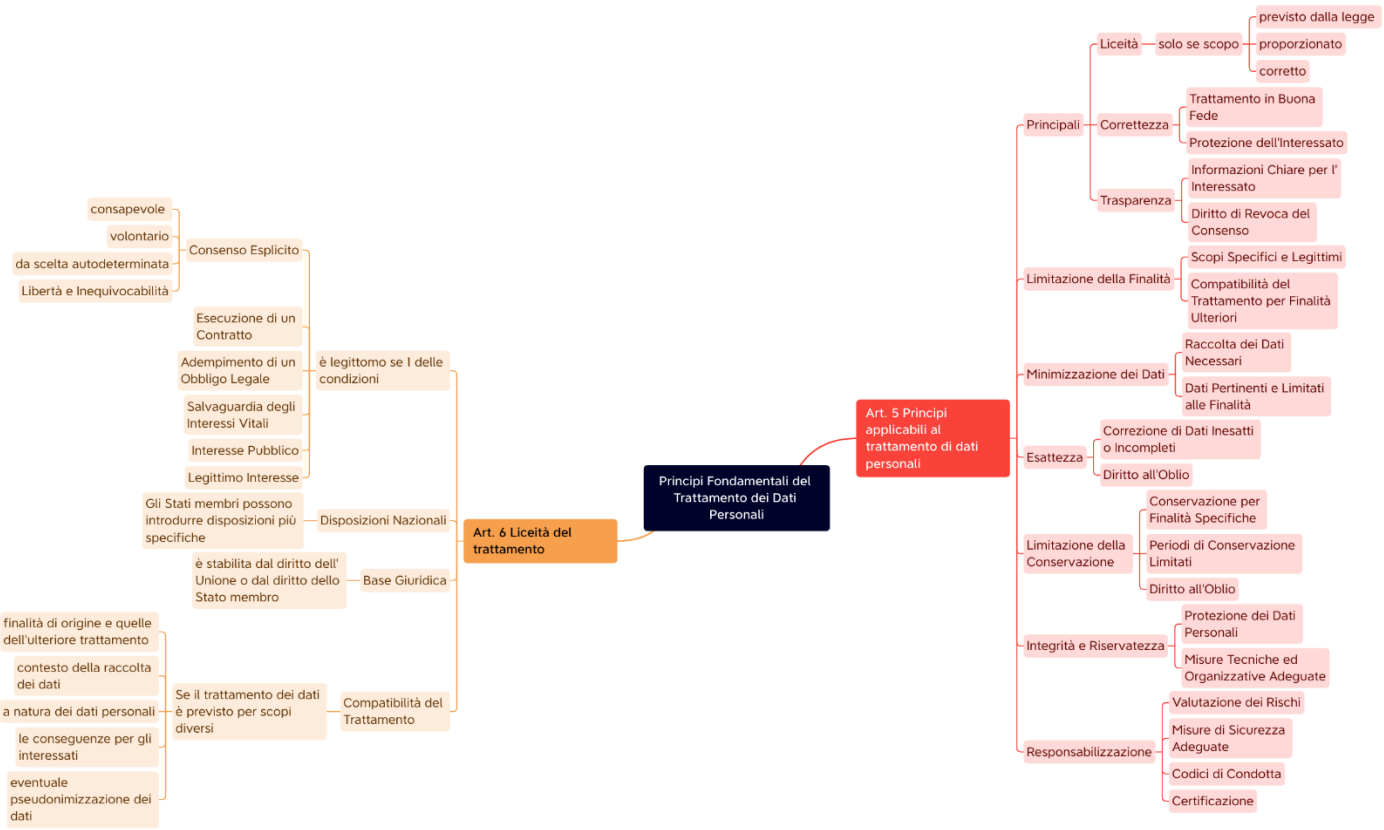
[161] GDPR art. 42 - Organismi di certificazione

[162] GDPR art. 32 - Sicurezza del trattamento, ove al punto 1 è stabilito: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso…*"

[163] Si veda: Capitolo terzo, L'accountability

legati all'obbligo di adottare misure tecniche e organizzative adeguate, dunque differenti di caso in caso, in base all'analisi e alla gestione dei rischi tipici associati all'attività di trattamento effettuata. Questi principi generali di prevenzione e precauzione contribuiscono a definire il rischio aziendale socialmente ed economicamente accettabile, anche alla luce dei principi di ragionevolezza e proporzionalità.

Mappa concettuale 11 - I principi fondamentali del trattamento dei dati personali



La responsabilità per trattamento illecito

Per affrontare questo tema, giova richiamare di nuovo l'articolo 82 del GDPR, ove è stabilito che:

> "C*hiunque subisca un danno materiale o immateriale causato da una violazione del presente regolamento ha il diritto di ottenere il risarcimento del danno dal titolare del trattamento o dal responsabile del trattamento*".

Un trattamento si considera illegittimo quando si verifica una delle seguenti situazioni[164]:

- è contrario alle leggi vigenti, rappresentando una condotta che viola il diritto;
- danneggia l'altrui situazione giuridica soggettiva tutelata dalla legge.

In caso di un trattamento illegittimo dei propri dati personali, il danneggiato ovvero l'interessato e/o chiunque ritenga di aver subito un danno[165], ha il diritto di richiedere il risarcimento di quanto subito e, come vedremo, l'espressione "*materiale o immateriale*" utilizzata dal Legislatore, è chiaramente riferita al danno patrimoniale e non patrimoniale. Questo risarcimento può essere richiesto sia in seguito a condotte del titolare del trattamento (e, se del caso, dei suoi co-titolari) che del responsabile del trattamento (e, se presenti, dei suoi co-responsabili e sub-responsabili). Il titolare è responsabile per i danni derivanti da un trattamento che viola il Regolamento, mentre il responsabile lo sarà solo per i danni derivanti da un inadempimento dei suoi obblighi specifici o per aver agito in modo contrario alle legittime istruzioni del titolare. Eventuali sub-responsabili, invece, rispondono solo all'interno di un rapporto contrattuale con il responsabile, dunque non direttamente verso gli interessati. In breve: sia il

[164] MAGRI G., MARTINELLI S. e THOBANI S., Manuale di diritto privato delle nuove tecnologie, Giappichelli, Torino, 2022, P. 204

[165] Si veda: Capitolo quarto - La responsabilità civile da illecito trattamento dei dati personali, Il Profilo soggettivo, La legittimazione attiva.

titolare che il responsabile sono i soggetti a responsabilità in caso di violazione delle disposizioni del GDPR.

Il Legislatore europeo, al Considerando n. 146 del GDPR, indica che il concetto di danno deve essere interpretato in senso ampio e, come si vedrà di seguito, lo fa sia per quanto riguarda il criterio di risarcibilità che per quanto riguarda il criterio di imputazione. Il Considerando afferma che:

> "*Il titolare del trattamento o il responsabile del trattamento dovrebbe risarcire i danni cagionati a una persona da un trattamento non conforme al presente regolamento ma dovrebbe essere esonerato da tale responsabilità se dimostra che l'evento dannoso non gli è in alcun modo imputabile. Il concetto di danno dovrebbe essere interpretato in senso lato alla luce della giurisprudenza della Corte di giustizia in modo tale da rispecchiare pienamente gli obiettivi del presente regolamento. Ciò non pregiudica le azioni di risarcimento di danni derivanti dalla violazione di altre norme del diritto dell'Unione o degli Stati membri. Un trattamento non conforme al presente regolamento comprende anche il trattamento non conforme agli atti delegati e agli atti di esecuzione adottati in conformità del presente regolamento e alle disposizioni del diritto degli Stati membri che specificano disposizioni del presente regolamento. Gli interessati dovrebbero ottenere pieno ed effettivo risarcimento per il danno subito. Qualora i titolari del trattamento o i responsabili del trattamento siano coinvolti nello stesso trattamento, ogni titolare del trattamento o responsabile del trattamento dovrebbe rispondere per la totalità del danno. Tuttavia, qualora essi siano riuniti negli stessi procedimenti giudiziari conformemente al diritto degli Stati membri, il risarcimento può essere ripartito in base alla responsabilità che ricade su ogni titolare del trattamento o responsabile del trattamento per il danno cagionato dal trattamento, a condizione che sia assicurato il pieno ed effettivo risarcimento dell'interessato che ha subito il danno. Il titolare del trattamento o il responsabile del trattamento che ha pagato l'intero risarcimento del danno può successivamente proporre un'azione di*

regresso contro altri titolari del trattamento o responsabili del trattamento coinvolti nello stesso trattamento".

Il Considerando n. 146 stabilisce quindi che il titolare o il responsabile del trattamento deve risarcire i danni causati a una persona da un trattamento non conforme al GDPR, a meno che non dimostri che l'evento dannoso non è riconducibile a lui. Il titolare/responsabile dovrà infatti provare:

1. che non c'è stata una violazione della normativa in materia di protezione di dati personali;
2. in caso di violazione, che l'evento dannoso non è in alcun modo a lui imputabile[166].

Ebbene, con riguardo a questo secondo punto, ci si domanda quali siano effettivamente gli elementi utilizzabili dal titolare/responsabile utili a dimostrare che "*…l'evento dannoso non gli è in alcun modo imputabile*".

Si tratta infatti di stabilire il criterio di imputazione, tema che verrà affrontato di seguito.

Il danno

Per richiedere il risarcimento del danno è essenziale innanzitutto che vi sia effettivamente un danno da risarcire ed è centrale è il principio che afferma che a carico del danneggiato grava l'onere della prova, come anche ribadito dalla Suprema Corte[167]. Egli, infatti, dovrà provare:

1. il trattamento riconducibile al titolare/responsabile;
2. il danno;
3. il nesso causale tra trattamento e danno.

Ciò significa che la violazione delle norme a tutela dei dati personali da sola non è sufficiente per una condanna al risarcimento; è necessario che il danneggiato

[166] GDPR art. 82 - Diritto al risarcimento e responsabilità, che al paragrafo 3 indica che: "*Il titolare del trattamento o il responsabile del trattamento è esonerato dalla responsabilità, a norma del paragrafo 2 se dimostra che l'evento dannoso non gli è in alcun modo imputabile.*"

[167] Corte di cassazione, sez. I, 07/10/2015, n. 20106 https://www.eius.it/giurisprudenza/2015/322

dimostri che ha effettivamente subito un danno[168]. Come affermato dalla Corte di cassazione, ad esempio, la semplice perdita di documentazione contenente dati personali, anche se sensibili, non comporta necessariamente un obbligo di risarcimento, a meno che non si dimostri che questa documentazione è caduta nelle mani di soggetti non autorizzati e abbia causato un danno ingiusto (dimostrabile)[169].

Il GDPR non fa distinzione tra danni patrimoniali e non patrimoniali, utilizzando invece la nozione di "*materiale o immateriale*"; vengono tuttavia specificati alcuni dettagli ai Considerando n. 75[170] e n. 85[171].

---

[168] MAGRI G., MARTINELLI S., THOBANI S., Manuale di diritto privato delle nuove tecnologie, Giappichelli, Torino, 2022, P. 208

[169] Corte di Cassazione, sez. VI, 11/01/2016, n. 222, https://renatodisa.com/corte-di-cassazione-sezione-vi-ordinanza-11-gennaio-2016-n-222-il-semplice-smarrimento-di-documenti-con-dati-supersensibili-da-parte-del-ministero-non-da-diritto-al-risarcimento-del-danno-se-manc/

[170] GDPR - Considerando n. 75: "*I rischi per i diritti e le libertà delle persone fisiche, aventi probabilità e gravità diverse, possono derivare da trattamenti di dati personali suscettibili di cagionare un danno fisico, materiale o immateriale, in particolare: se il trattamento può comportare discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo; se gli interessati rischiano di essere privati dei loro diritti e delle loro libertà o venga loro impedito l'esercizio del controllo sui dati personali che li riguardano; se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza; in caso di valutazione di aspetti personali, in particolare mediante l'analisi o la previsione 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, al fine di creare o utilizzare profili personali; se sono trattati dati personali di persone fisiche vulnerabili, in particolare minori; se il trattamento riguarda una notevole quantità di dati personali e un vasto numero di interessati.*"

[171] GDPR - Considerando n. 85: "*Una violazione dei dati personali può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata. Pertanto, non appena viene a conoscenza di un'avvenuta violazione dei dati personali, il titolare del trattamento dovrebbe notificare la violazione dei dati personali all'autorità di controllo competente, senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che il titolare del trattamento non sia in grado di dimostrare che,*

I danni di natura patrimoniale, ovvero quelli con un impatto di natura economica, devono anch'essi essere provati dal danneggiato. Ad esempio, nel caso in cui un individuo subisca discriminazioni nell'accesso a un servizio o all'occupazione a causa di una profilazione illegittima, o ancora, laddove vadano persi dati personali che sono cruciali per la professione dell'interessato.

Sono altrettanto rilevanti i danni non patrimoniali, per la cui definizione in genere ci si basa su una classificazione di singole ipotesi, tra cui il danno biologico, il danno morale e il danno esistenziale. Il danno biologico è definito nel codice delle assicurazioni come una lesione temporanea o permanente all'integrità psico-fisica della persona che influisce negativamente sulle attività quotidiane e sugli aspetti dinamico-relazionali della vita del danneggiato. Il danno morale si riferisce alla sofferenza soggettiva causata da un fatto illecito, che può essere di natura transitoria o permanente. Il danno esistenziale è qualsiasi compromissione delle attività realizzatrici della persona umana, come la lesione della serenità familiare o del godimento di un ambiente salubre. Si distingue dal danno biologico poiché non presuppone una lesione fisica e dal danno morale poiché non costituisce una sofferenza di tipo soggettivo. In generale, i danni non patrimoniali consistono in una privazione, o anche semplicemente in una riduzione, di un valore personale che non è direttamente misurabile in termini economici. Dunque, si tratta di danni sicuramente più complessi da dimostrare, valutare e quantificare, consistendo in disagi, fastidi e disturbi come conseguenze di un trattamento illecito di dati. Questi disagi possono derivare da violazioni delle norme di trattamento dei dati personali, ma non necessariamente da lesioni dei diritti della personalità tradizionali come la reputazione, la riservatezza o l'identità personale.

Va notato, tuttavia, che la giurisprudenza ammette il risarcimento dei danni non patrimoniali solo laddove essi superino una certa soglia di gravità ovvero se

---

conformemente al principio di responsabilizzazione, è improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Oltre il termine di 72 ore, tale notifica dovrebbe essere corredata delle ragioni del ritardo e le informazioni potrebbero essere fornite in fasi successive senza ulteriore ingiustificato ritardo."

possano essere considerati "*seri*". Tale approccio, tratto dal principio di solidarietà di cui all'art. 2 della nostra Costituzione, prevede che non tutti i disagi, fastidi e sensazioni spiacevoli derivanti da un trattamento illecito dei dati possono giustificare un risarcimento e prevede altresì che il danno non patrimoniale può essere risarcito solo se comporta un effettivo e significativo pregiudizio.

Il concetto di danno, come delineato nel Considerando n. 146 del Regolamento, dovrà essere interpretato in modo ampio, nel rispetto degli obiettivi del GDPR, con particolare attenzione alla protezione degli interessi dell'individuo.

A tal riguardo, la giurisprudenza nazionale è giunta in soccorso in varie occasioni, come nel 2014 con la sentenza del caso della pubblicazione sul sito di una Università dei dati anagrafici degli studenti[172] in cui la Corte di cassazione si è espressa esponendo il seguente principio di diritto:

> "*Il danno non patrimoniale risarcibile ai sensi del D.lgs. 30 giugno 2003, n. 196, art. 15, (c.d. codice della privacy) non si sottrae alla verifica di "gravità della lesione" (concernente il diritto fondamentale alla protezione dei dati personali, quale intimamente legato ai diritti ed alle libertà indicate dall'art. 2 del codice, convergenti tutti funzionalmente alla tutela piena della persona umana e della sua dignità) e di "serietà del danno" (quale perdita di natura personale effettivamente patita dall'interessato), che, in linea generale, si richiede in applicazione dell'art. 2059 c.c., nelle ipotesi di pregiudizio inferto ai diritti inviolabili previsti in Costituzione. Ciò in quanto, anche nella fattispecie di danno non patrimoniale di cui al citato art. 15, opera il bilanciamento (siccome pienamente consentito all'interprete dal modo in cui si è realizzata nello specifico l'interpositio legislatoris) del diritto tutelato da detta disposizione con il principio di solidarietà - di cui il principio di tolleranza è intrinseco precipitato -, il quale, nella sua immanente configurazione, costituisce il punto di*

[172] Corte di cassazione, 15.7.2014, n. 16133 https://www.altalex.com/documents/news/2014/10/09/privacy-violazione-danno-non-patrimoniale-risarcibilita-soglia-minima

mediazione che permette all'ordinamento di salvaguardare il diritto del singolo nell'ambito di una concreta comunità di persone che deve affrontare i costi di una esistenza collettiva."

La suprema Corte ha infatti concluso che solo una lesione che: "*…offenda in modo sensibile (e cioè oltre la soglia di tollerabilità) la sua [della normativa in materia di protezione di dati personali] portata effettiva*" giustifica un risarcimento. Questa sentenza chiarisce che quando si tratta di risarcire il danno non patrimoniale causato da una violazione della privacy, la gravità della lesione subita e la serietà del danno devono essere attentamente valutate. Ciò conferma che non tutti i casi di violazione della privacy comporteranno necessariamente un risarcimento, ma solo quelli in cui si può dimostrare che la lesione è significativa e che si è verificato un danno effettivo alla persona coinvolta. Inoltre, la sentenza sottolinea l'importanza del bilanciamento tra il diritto individuale alla protezione dei dati personali e il principio di solidarietà all'interno della comunità.

Analogamente, nel 2017, un ulteriore intervento della giurisprudenza nazionale circa l'interpretazione del concetto di danno è rappresentato dal caso in cui la Società Italiana degli Avvocati Amministrativisti (SIAA), che ha estratto l'indirizzo e-mail del Sig. S.G. dagli elenchi conservati presso l'Ordine degli Avvocati di Milano, ha utilizzato quest'indirizzo per inviare al Sig. S.G. messaggi di posta elettronica a scopo pubblicitario, senza ottenere il previo consenso[173]. Il Sig. S.G. ha chiesto ripetutamente al titolare del trattamento della SIAA di interrompere l'invio di tali comunicazioni indesiderate[174]. Poiché tali richieste sono rimaste inefficaci, il Sig. S.G. ha citato in giudizio la SIAA chiedendo un risarcimento danni di 360€[175]. Nel corso del processo di primo grado, nel quale

[173] Corte di cassazione, sez. I, 08/02/2017, n. 3311 https://sentenze.laleggepertutti.it/sentenza/cassazione-civile-n-3311-del-08-02-2017

[174] Si veda: Capitolo Quarto - La responsabilità civile da illecito trattamento dei dati personali, La tutela rimediale, La tutela in autonomia.

[175] Si veda: Capitolo Quarto - La responsabilità civile da illecito trattamento dei dati personali, La tutela rimediale, La tutela giurisdizionale.

è emerso che S.G. aveva ricevuto soltanto dieci e-mail pubblicitarie nel corso di tre anni, il tribunale ha respinto la richiesta di risarcimento, motivando che non era stato dimostrato né l'esistenza del danno né la sua entità. Il Sig. S.G. ha poi presentato un ricorso in Cassazione, sostenendo che il giudice aveva erroneamente applicato l'articolo 2043[176] del Codice civile anziché l'articolo 2050[177]. La Suprema Corte, a prescindere dalla richiesta, ha respinto il ricorso sostenendo che il tribunale aveva in ogni caso correttamente applicato il principio secondo cui il danno non patrimoniale derivante da un trattamento illecito dei dati personali deve essere valutato in base alla gravità della lesione subita e alla serietà del danno. Il diritto al risarcimento sorge solamente in caso di una "*lesione ingiustificabile*" del "*diritto fondamentale alla protezione dei dati personali*", che non è causata da una "*semplice violazione delle disposizioni contenute nell'articolo 11 del Codice della privacy*", ma piuttosto da "*un'offesa che ne comprometta in modo significativo la portata effettiva*".

La valutazione del danno non patrimoniale è stata basata su elementi quali "*fastidio e turbamento dovuti alla plurima ricezione di materiale pubblicitario e promozionale non desiderato*", "*danno esistenziale*", e "*danno alla vita di relazione*", causati dallo "*stress e alle sofferenze morali cagionate dalle indebite e continue interferenze*". È importante notare che la sentenza in questione non pare entrare in conflitto con le decisioni precedenti che riconoscono il risarcimento del danno in casi simili. Piuttosto, precisa che, in linea di principio, l'invio di comunicazioni indesiderate potrebbe sì causare un danno ingiusto risarcibile, ma nel caso specifico delle dieci e-mail pubblicitarie inviate nel corso di tre anni, mancano una "*lesione grave*" e un "*danno serio*".

Con questa sentenza la Corte conferma la sua precedente giurisprudenza in materia di risarcimento del danno non patrimoniale derivante da illecito

[176] Codice civile art. 2043 - Risarcimento per fatto illecito: "*Qualunque fatto doloso o colposo, che cagiona ad altri un danno ingiusto, obbliga colui che ha commesso il fatto a risarcire il danno*"

[177] Codice civile art. 2050 - Responsabilità per l'esercizio di attività pericolose: "*Chiunque cagiona danno ad altri nello svolgimento di un'attività pericolosa, per sua natura o per la natura dei mezzi adoperati, è tenuto al risarcimento, se non prova di avere adottato tutte le misure idonee a evitare il danno.*"

trattamento dei dati personali. Infatti, viene richiamato lo stesso approccio del sopracitato caso dell'università che ha pubblicato informazioni personali di centinaia di studenti. L'argomentazione di entrambe le sentenze si basa, dunque, sulla non gravità della lesione e sulla non serietà del danno cagionato; nel primo caso per la pubblicazione di informazioni personali, nel secondo per l'invio di e-mail indesiderate.

Ed ancora, lo scorso maggio 2023, al riguardo si è espressa anche la Corte di giustizia europea relativamente ad un caso riguardante l'elaborazione automatizzata ed illecita profilazione da parte di un titolare/responsabile di dati relativi alle preferenze politiche di un interessato[178]. Il contenzioso riguardava il Sig. UI e la Österreichische Post AG, in relazione al reclamo (una domanda di pronuncia pregiudiziale alla CDGUE circa sull'interpretazione dell'articolo 82 del GDPR) presentato dal Sig. UI, con l'obiettivo di ottenere un risarcimento per il danno morale che sostiene di aver subito a causa dell'elaborazione da parte di tale società di dati relativi alle preferenze politiche di persone residenti in Austria, tra cui lui stesso, senza il suo consenso. Il Giudice del rinvio nella sua pronuncia iniziale aveva sottolineato che:

> *"…il considerando 146 del GDPR raccomanda un'interpretazione estensiva della nozione di «danno», ai sensi di tale regolamento. Esso ritiene che un danno immateriale debba essere risarcito, in forza dell'articolo 82 di quest'ultimo, se è tangibile, quand'anche fosse lieve. Per contro, un danno del genere non dovrebbe essere risarcito qualora risultasse del tutto trascurabile, come avverrebbe in presenza dei semplici sentimenti sgradevoli che accompagnano abitualmente una siffatta violazione*."

Tuttavia, invece, nel maggio del 2023 la Corte di giustizia europea si esprime con una sentenza e dichiara che:

> "*1) L'articolo 82, paragrafo 1, del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla*

[178] Corte di Giustizia UE, 4.5.2023, C 300/21
https://eur-lex.europa.eu/legal-content/IT/TXT/HTML/?uri=CELEX:62021CJ0300

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), deve essere interpretato nel senso che: la mera violazione delle disposizioni di tale Regolamento non è sufficiente per conferire un diritto al risarcimento.

2) L'articolo 82, paragrafo 1, del Regolamento 2016/679 deve essere interpretato nel senso che: esso osta a una norma o una prassi nazionale che subordina il risarcimento di un danno immateriale, ai sensi di tale disposizione, alla condizione che il danno subito dall'interessato abbia raggiunto un certo grado di gravità.

3) L'articolo 82 del Regolamento 2016/679 deve essere interpretato nel senso che: ai fini della determinazione dell'importo del risarcimento dovuto in base al diritto al risarcimento sancito da tale articolo, i giudici nazionali devono applicare le norme interne di ciascuno Stato membro relative all'entità del risarcimento pecuniario, purché siano rispettati i principi di equivalenza e di effettività del diritto dell'Unione."

Questa recente sentenza sottolinea che il GDPR impone restrizioni all'accesso al risarcimento per violazioni delle norme sulla protezione dei dati; tuttavia, non è richiesto un elevato livello di gravità per pretendere il risarcimento per danni immateriali. La nuova decisione della Corte di giustizia europea sembra indirizzare la ricerca di un equilibrio tra due elementi:

1. la necessità di garantire il rispetto delle norme sulla protezione dei dati;
2. la giustezza (equivalenza ed effettività) del risarcimento nei casi di violazione.

Al punto 1 la Corte specifica che il semplice fatto di violare le regole del GDPR non è sufficiente per far scattare il diritto al risarcimento. Questo punto è in linea con la giurisprudenza nazionale; in altre parole: se un'organizzazione o un individuo tratta i dati personali in violazione del GDPR, ciò non implica automaticamente che chi ha subito il danno abbia diritto a un risarcimento. Per ottenere un risarcimento, è necessario dimostrare ulteriori circostanze, come

l’esistenza di un danno effettivo e il collegamento causale tra la violazione e il danno subito.

Al punto 2 la Corte afferma tuttavia che il GDPR non consente alle norme o alle pratiche nazionali di subordinare il risarcimento per un danno immateriale alla condizione che il danno subito abbia raggiunto un certo grado di gravità. Questo pare discostarsi dalla giurisprudenza nazionale e significa che il GDPR riconosce la possibilità di richiedere il risarcimento per danni immateriali senza specificare un livello di gravità. In altre parole, la Corte europea afferma che anche danni immateriali di minore entità possono rientrare nella sfera di applicazione del GDPR, tuttavia essi devono derivare da una violazione delle norme sulla protezione dei dati.

Infine, al punto 3, la decisione della Corte europea conferma il ruolo degli Stati membri nell'applicazione del GDPR, affermando che giudici nazionali devono applicare le norme interne degli Stati membri: per calcolare l'importo del risarcimento dovuto in base all'articolo 82 del GDPR, i tribunali nazionali di ciascuno Stato membro devono fare riferimento alle leggi nazionali relative all'entità del risarcimento pecuniario. In altre parole, il modo in cui viene determinato l'importo del risarcimento dovuto per una violazione delle norme sulla protezione dei dati può variare da uno Stato membro all'altro, a condizione che sia conforme al diritto dell'Unione Europea. Allo stesso punto 3 viene chiarita un’ulteriore condizione importante: i giudici deli Stati membri devono assicurarsi che le norme nazionali siano conformi ai principi di equivalenza e di effettività del diritto dell'Unione europea. Ciò significa che, da un lato gli Stati membri hanno una certa flessibilità nel determinare l'entità del risarcimento, dall’altro devono però farlo in modo da garantire che i diritti e le protezioni offerti dal GDPR siano mantenuti e rispettati in maniera efficace ed equa[179].

[179] IERMANO A., I principi di equivalenza ed effettività tra autonomia procedurale e 'limiti' alla tutela nazionale, in Il Diritto dell'Unione europea, Giappichelli, 2019: *“…gli Stati sono “autonomi” nei “limiti” fissati dai principi di equivalenza ed effettività, i quali a loro volta rispondono al “limite” ad essi sovraordinato di garantire sempre e comunque l’attuazione effettiva del diritto dell’Unione europea.*”

Il criterio di imputazione

Uno dei casi in cui il titolare o il responsabile possono essere esenti da responsabilità, si verifica quando essi riescono a dimostrare che il danno è stato causato da un evento casuale/accidentale o da una circostanza inevitabile che interrompe il nesso causale. La prova di un caso fortuito o di forza maggiore, quindi, pare costituire una valida esenzione dalla responsabilità.

Una seconda possibilità di esenzione da responsabilità del titolare o del responsabile è la circostanza in cui essi riescano a fornire prova di aver adottato tutte le misure adeguate previste dal GDPR, il che richiama implicitamente -di nuovo- il principio dell'accountability. Si potrebbe pertanto avanzare -con prudenza- l'ipotesi che attraverso l'implicito riferimento all'accountability, l'art. n. 82 possa "raccordare" tutti gli altri articoli in cui vengono richiamati principi di auto-responsabilizzazione, autonomia, trasparenza, ragionevolezza e proporzionalità.[180]

Questo concetto di danno, interpretato dalla giurisprudenza in senso ampio alla luce del Considerando n. 146 del GDPR, è ben rappresentato da una sentenza della Corte di cassazione assai recente (maggio 2023) che riguarda la

---

https://www.dirittounioneeuropea.eu/Tool/NewsletterArchive/Detail/view_html?id_newsletter=19&anno=2019

[180] GDPR art. 24 - Responsabilità del titolare del trattamento: "*Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario*."

GDPR art. 28 - Responsabile del trattamento: "*Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato*."

GDPR art. 32 - Sicurezza del trattamento: "*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.*"

pubblicazione su internet di dati personali di un dipendente comunale relativi al pignoramento del proprio stipendio[181]. il Comune in questione ha presentato un ricorso in cassazione contro la sentenza del Tribunale di Roma che lo aveva condannato a risarcire i danni causati a un dipendente a causa di un trattamento illecito dei suoi dati personali. Il ricorso è basato su diversi motivi, tra cui la violazione del GDPR e l'art. 2050 del Codice civile italiano. Il Comune ha affermato che il trattamento illecito dei dati del Sig. A.A. è avvenuto per errore umano e che non dovrebbe essere considerato come causa di danno. Tuttavia, il tribunale ha stabilito che il trattamento era in ogni caso illecito e che il danno era stato effettivamente subito dal Sig. A.A. Il GDPR stabilisce il diritto a ottenere il risarcimento per il danno causato da una violazione del Regolamento, anche se la lesione è marginale; inoltre, il concetto di danno è interpretato in senso ampio e include danni materiali e immateriali. Il tribunale ha ritenuto che il trattamento illecito dei dati del Sig. A.A. abbia causato un danno immateriale in relazione alla protezione dei dati personali:

> "…*l'esclusione del principio del danno in re ipsa presuppone, in questi casi, la prova della serietà della lesione conseguente al trattamento; ciò vuol dire che può non determinare il danno la mera violazione delle prescrizioni formali in tema di trattamento del dato, mentre induce sempre al risarcimento quella violazione che concretamente offenda la portata effettiva del diritto alla riservatezza*".

Il ricorso del Comune è stato respinto, confermando che il titolare del trattamento è tenuto a risarcire il danno causato (che evidentemente è stato dimostrato ed anche ritenuto evidente) da un trattamento non conforme al GDPR. Anche in questo caso il concetto di danno è stato interpretato in senso ampio alla luce del Considerando n. 146 del GDPR, e il fatto che il trattamento sia avvenuto per errore umano non esonera il titolare del trattamento dalla propria responsabilità. In particolare, il Giudice non ha -a parer dello scrivente,

[181] Corte di cassazione civile sez. I, 12/05/2023, n. 13073 https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/QUOTIDIANI_VERTICALI/Online/_Oggetti_Embedded/Documenti/2023/05/30/Cass%2013073_2023.pdf

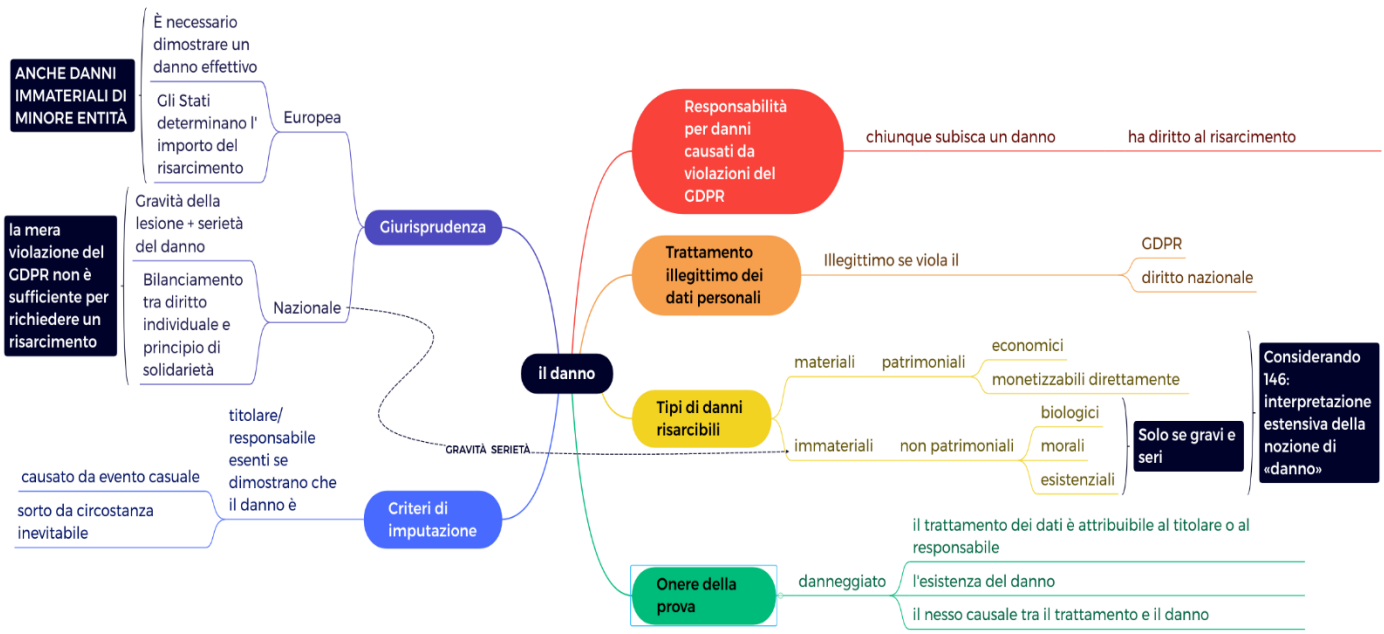
correttamente- valutato l'errore umano come "*caso fortuito*" o "*di forza maggiore*", tantomeno come evento non imputabile al Titolare. In definitiva, nella valutazione del titolo di imputazione, viene stabilita la colpa del titolare/responsabile in ragione della negligenza nell'aver commesso l'errore, che -come già detto, ancorché involontario- non lo ha liberato dalla responsabilità.

Il costante riferimento al principio di accountability sottolinea in maniera inequivocabile l'importanza che il Legislatore ha attribuito alla necessità di garantire sempre un elevato standard di responsabilità in tutte le circostanze. Le organizzazioni devono essere proattive nel prevedere, identificare e mitigare i rischi, implementando politiche e procedure robuste per garantire la sicurezza dei dati personali.

Il GDPR, pur ammettendo l'esistenza di situazioni occasionali che possono persino arrivare ad esonerare il titolare/responsabile dalle proprie responsabilità, insiste in modo inequivocabile sull'adozione di misure "idonee" atte a gestire anche eventuali errori e le conseguenti violazioni delle norme sulla protezione dei dati.

L'accountability non è quindi solo una questione formale, ma un principio sostanziale che richiede un impegno concreto nell'assicurare la protezione dei dati e permea l'intero GDPR rappresentandone le fondamenta.

Mappa concettuale 12 – Il danno



Conclusioni

Il panorama del GDPR e il principio dell'accountability

Il 2018, con l'entrata in vigore del General Data Protection Regulation, ha segnato una svolta importante nella protezione dei dati personali.
Il principio fondamentale che caratterizza il GDPR è l'accountability, una vera e propria innovazione, che può essere considerata il pilastro di questo cambiamento: non più regole ex-ante stringenti, rigide, ma un nuovo e moderno approccio flessibile e adattabile, che richiede ai titolari del trattamento dei dati e ai responsabili di valutare, decidere e creare le condizioni per garantire la piena conformità del trattamento alle disposizioni del Regolamento. Questo approccio rappresenta un cambiamento sostanziale rispetto alla precedente disciplina, contenuta nella precedente Direttiva 95/46/CE, ed è fondamentale per la protezione dei diritti fondamentali degli interessati sempre più spesso influenzati dai rapidi cambiamenti della società moderna. L'accountability non è solo una questione di conformità formale, ma comporta una profonda trasformazione anche culturale nell'approccio e di formazione interna; richiede infatti una consapevolezza attiva ed una nuova conoscenza da parte delle organizzazioni che operano con dati personali, indirizzandole a integrare e modernizzare la protezione dei dati in tutte le loro attività, strumenti ICT e processi. Questo principio, inoltre, mette in evidenza l'importanza di riconoscere la sensibilità e il grande valore che hanno i dati personali, adottando misure rigorose, ma allo stesso tempo moderne e flessibili a garanzia di sicurezza e integrità.

Responsabilità e risarcimento per violazioni del GDPR

Un elemento chiave del GDPR è l'istituzione del diritto al risarcimento per chi subisce un danno ingiusto derivante da una violazione del GDPR. Questa responsabilità oggettiva pone il peso della dimostrazione di un corretto

trattamento che grava sul titolare del trattamento e sul responsabile del trattamento. Se il trattamento dei dati è illegittimo e ha causato un danno, il risarcimento deve essere concesso. Tuttavia, il concetto di *danno* è assai ampio e flessibile, e comprende sia danni materiali facilmente monetizzabili, che quelli immateriali. La giurisprudenza italiana ha stabilito che il risarcimento non è dovuto automaticamente in caso di violazione del GDPR; il danno deve innanzitutto esistere ed essere dimostrato, e dovrà anche superare una soglia di gravità e di serietà. Questa interpretazione della giurisprudenza evita richieste di risarcimento per violazioni minori e si concentra sui casi in cui vi sia un danno effettivo.

Tuttavia, la giurisprudenza europea nel 2023 ha invece fissato nuovi parametri stabilendo che il risarcimento per violazioni del GDPR non è automatico, ma soprattutto che esso non è subordinato alla condizione che il danno subito sia grave ed infine che gli Stati membri sono autonomi nella quantificazione del risarcimento, seppur nel rispetto dei principi equivalenza ed effettività del diritto unionale.

Elemento cruciale nella valutazione del risarcimento del danno è il bilanciamento tra il diritto individuale alla protezione dei dati personali e il principio di solidarietà all'interno della comunità[182]. Questo bilanciamento è fondamentale per evitare eccessive richieste di risarcimento che potrebbero rendere insostenibile la conformità al GDPR. Tale equilibrio è in linea con l'obiettivo del GDPR di trovare un bilanciamento tra la protezione dei diritti individuali, da un lato, e la libera circolazione dei dati dall'altro.

In ultima analisi, il GDPR, grazie al ruolo centrale del principio dell'accountability nella responsabilità per il trattamento illecito dei dati personali, ha successo nel conciliare questi obiettivi, garantendo un'adeguata protezione dei dati personali senza tuttavia prevedere limitazioni e imposizioni eccessive.

[182] Costituzione della Repubblica Italiana - Principi fondamentali, art. 2: *"La Repubblica riconosce e garantisce i diritti inviolabili dell'uomo, sia come singolo, sia nelle formazioni sociali ove si svolge la sua personalità, e richiede l'adempimento dei doveri inderogabili di solidarietà politica, economica e sociale."*

Prospettive future: l'influenza del GDPR

Osservando le prospettive future della protezione dei dati personali in Europa, emerge un quadro interessante. In questi anni abbiamo assistito a un rafforzamento sia a livello normativo che nell'applicazione pratica della tutela amministrativa e giurisdizionale dei dati personali. Questo sviluppo mira a garantire un'interpretazione uniforme del concetto europeo di protezione dei dati, basandosi principalmente sull'interazione concreta tra le autorità di controllo. Il sistema di salvaguardia è integrato e punta a garantire una visione condivisa della protezione dei dati personali, consentendo al contempo alcune flessibilità per adattarsi alle specificità dei diversi sistemi giuridici presenti nell'Unione europea.

Inoltre, sia a livello nazionale che europeo, il diritto alla protezione dei dati personali è posto in cima alla piramide della gerarchia delle fonti normative: a livello nazionale, ha una rilevanza costituzionale, mentre a livello europeo, oltre -naturalmente- ad essere richiamato nella Carta dei diritti fondamentali dell'Unione europea (Carta di Nizza),[183] è anche esplicitamente menzionato in una delle fonti di diritto primario, ovvero dal TFUE[184] all'articolo n. 16[185]. Questa

[183] Carta dei diritti fondamentali dell'Unione europea art. 8 - Protezione dei dati di carattere personale, che afferma: "*1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Tali dati devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge. Ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica. 3. Il rispetto di tali regole è soggetto al controllo di un'autorità indipendente.*"

[184] TFUE - Trattato sul funzionamento dell'Unione europea, fonte primaria del diritto dell'Unione europea (assieme al TUE - Trattato dell'Unione europea, ai Protocolli e agli Allegati).

[185] Trattato sul funzionamento dell'Unione europea, art. 16 *"1. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano. 2. Il Parlamento europeo e il Consiglio, deliberando secondo la procedura legislativa ordinaria, stabiliscono le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte delle istituzioni, degli organi e degli organismi dell'Unione, nonché da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del diritto dell'Unione, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità*

configurazione giuridica con il riconoscimento sia a livello nazionale che europeo, prevede che, per affrontare i futuri problemi legati alla protezione dei dati personali tra i Paesi membri dell'Unione europea, è necessario adottare una prospettiva multilivello. Ad esempio, con il crescente impatto dei Big Data o dell'IoT[186], è necessaria una regolamentazione pubblica per prevenire e contrastare il trattamento illecito dei dati personali, soprattutto considerando la natura extra territoriale della rete.

La domanda che sorge è se l'Unione europea sarà in grado di competere a livello globale con i modelli alternativi di protezione dei dati personali adottati da altre superpotenze e come affronterà gli interessi privati delle grandi aziende multinazionali del settore informatico. L'Unione europea sembra, a parere dello scrivente, avere il potenziale per emergere come leader nella protezione dei dati personali, com'è dimostrato dall'influenza esercitata a livello internazionale grazie al GDPR e, più di recente, attraverso il Regolamento UE 2022/868, meglio noto come DGA - Data Governance Act, che definisce le regole per favorire la condivisione dei dati all'interno dell'Unione -a vantaggio di imprese e cittadini- attraverso[187]:

1. il riutilizzo dei dati pubblici;
2. i servizi di intermediazione di dati;
3. l'altruismo dei dati.

Tuttavia, per essere davvero un punto di riferimento nella difesa dei diritti, l'Unione europea deve garantire un'applicazione uniforme della nozione di protezione dei dati personali in tutti i paesi membri, affinché questa appaia coerente sulla scena internazionale.

---

indipendenti. Le norme adottate sulla base del presente articolo fanno salve le norme specifiche di cui all'articolo 39 del trattato sull'Unione europea."

[186] Si veda: Capitolo Secondo - La storia del diritto alla privacy, L'era dell'ICT.

[187] AgID, Cosa prevede il DGA https://www.agendadigitale.eu/sicurezza/privacy/la-data-economy-alla-prova-del-data-governance-act-lo-scenario/#:~:text=Il%20Regolamento%20UE%202022%2F868,%2C%20l'altruismo%20dei%20dati.

Dunque, il GDPR non è solo una norma europea, ma ha anche un'influenza globale su altre nazioni e culture: la giurisprudenza europea avrà un impatto significativo su come queste leggi vengono interpretate e applicate a livello globale. Pertanto, è verosimile anche aspettarsi che le conclusioni e le interpretazioni derivanti dai casi giuridici legati al GDPR influenzeranno il diritto alla privacy dei dati a livello internazionale.

Il panorama descritto rivela una sfida significativa anche per le organizzazioni che operano con dati personali nell'era del GDPR giacché gli obblighi dettati dalle Norme e il principio dell'accountability stanno spingendo le imprese a rivedere le loro pratiche di gestione dei dati. Il GDPR è il nuovo modo di pensare alla privacy dei dati personali e rappresenta una svolta culturale perché spinge le organizzazioni a riconoscere il valore intrinseco dei dati personali e a impegnarsi attivamente per proteggerli.

Il ruolo delle autorità di regolamentazione è cruciale in questo contesto, in particolare per garantire che il GDPR sia applicato in modo coerente e giusto, proteggendo gli interessati senza però creare oneri insostenibili per le organizzazioni. La chiarezza e la coerenza delle direttive emanate da queste autorità saranno fondamentali per una corretta applicazione del GDPR.

La sfida globale

Il Regolamento UE 2016/679 è stato un punto di svolta per la protezione dei dati personali; è nato in Europa, ma la sua influenza è destinata ad estendersi ben oltre i confini del continente e potrebbe rappresentare un nuovo punto di riferimento nel panorama giuridico mondiale, con l'ambizione di orientare un miglioramento globale della protezione dei dati basata sul pieno rispetto dei diritti individuali. La sua portata è senza precedenti, e la vera sfida del futuro è mantenere il delicato equilibrio tra il diritto alla privacy individuale e la responsabilità delle organizzazioni, con un occhio attento al futuro e alla solidarietà sociale. Mentre è fondamentale proteggere la privacy dei dati, non è opportuno dar seguito a richieste eccessive di risarcimento: questa è una sfida che riguarda l'intero pianeta, poiché la tutela dei dati sta diventando d'interesse globale. Gli Stati Uniti, che hanno storicamente iniziato il dibattito sulla privacy dei dati già dall'800, stanno osservando con attenzione l'evoluzione europea.

Il futuro dell'Europa nella protezione dei dati rappresenta una sfida globale, e come Unione, abbiamo l'opportunità di guidare "il cambiamento". Questa guida dovrà essere equa e bilanciata, pronta a rispettare i diritti individuali senza opprimere le organizzazioni, anche e soprattutto nel rispetto delle diverse culture, religioni e storia. La giurisprudenza europea avrà un ruolo cruciale nell'indicare la via da seguire, orientando gli attori globali nell'attuazione di un dialogo costruttivo al fine di sviluppare una protezione dei dati equa ed efficace a livello mondiale.

Bibliografia

BARBA A. E PAGLIANTINI S., Commentario del Codice civile delle persone, leggi correlate Vol. II, UTET giuridica, Roma, 2019

CAPANO, G., GUALMINI, E., Le pubbliche amministrazioni in Italia, Il Mulino, Bologna, 2011

CATERINA R., THOBANI S., Giurisprudenza Italiana - Diritto civile, Il diritto al risarcimento dei danni, UTET giuridica, 2019

CONTALDI G., Diritto europeo dell'economia, CyberLaws, Torino, 2019

CORTE COSTITUZIONALE, I diritti fondamentali nella Giurisprudenza della Corte costituzionale - Relazione predisposta in occasione dell'incontro della delegazione della Corte costituzionale con il Tribunale costituzionale della Repubblica di Polonia, Varsavia, 2006

D'AVANZO W., La tutela dei dati personali dopo il Regolamento europeo 679/2016, Mantova, 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, I confini del Digitale - Nuovi scenari per la protezione dei dati, Roma, 2019

GIROTTI, F., Amministrazioni Pubbliche, Carocci, Roma, 2007

MAGRI G., MARTINELLI S., THOBANI S., Manuale di diritto privato delle nuove tecnologie, Giappichelli, Torino, 2022

MORIGGI A., Regolamento generale sulla protezione dei dati UE 2016/679 - Versione multilingue con traduzione a fronte, Giappichelli, Milano, 2020

RAMACCIONI G., La protezione dei dati personali e il danno non patrimoniale, Jovene, Napoli, 2017

RODOTÀ S., Tecnopolitica - La democrazia e le nuove tecnologie della comunicazione, Laterza, Roma, 2004

THOBANI S., Protezione dei dati personali, in Giurisprudenza Italiana dal 1849 - UTET giuridica, 2019, P. 41-46

THOBANI S., Invio di comunicazioni indesiderate: il risarcimento del danno non patrimoniale, in Giurisprudenza Italiana dal 1849 - UTET giuridica, 2019, P. 1539-1545

THOBANI S., Il diritto dell'informazione e dell'informatica - I danno non patrimoniale da trattamento illecito dei dati personali (estratto), Guiffrè, Milano, 2017

TORRENTE A., SCHLESINGER P., Manuale di diritto privato, Varese, 2019

TOSI E., Responsabilità civile per illecito trattamento dei dati personali e danno non patrimoniale, Milano, 2019

VILLANI U., Istituzioni di Diritto dell'Unione europea, VI edizione, Cacucci, Bari, 2020

WARREN S.D. - BRANDEIS L.D., The Right to Privacy, USA, 1890

Ringraziamenti

Ringrazio la mia adorata Tiziana, che ho il privilegio di avere come moglie e che stimo tanto: paziente, saggia, straordinaria; mi ha sempre supportato anche in questa avventura e che soprattutto ha dovuto subire le "ripetute" ad alta voce pre-esame di tutti gli insegnamenti, arrivando a livelli di conoscenza che quasi le avrebbero consentito di sostenere gli esami.

Un grazie va ai miei figli Gabriele e Roberta che, senza rendersene conto, sono stati per me fonte di ispirazione nella decisione iniziale e di motivazione durante il percorso.

Ringrazio gli amici Daniela ed Emanuele, senza i quali non avrei mai scoperto UnitelmaSapienza e forse non avrei mai trovato la spinta necessaria per iscrivermi davvero all'Università, riprendendo i libri dopo oltre 30 anni.
Un ringraziamento va ancora agli amici Sara e Andrea, che hanno assistito alle diverse fasi della mia preparazione agli esami, sopportandomi e talvolta sacrificando il loro tempo libero. In particolare, un pensiero è dedicato ad Andrea, che con i suoi tentativi di incoraggiamento, come "...se non torni con la lode, non mi chiamare nemmeno," oppure "...mhh, bravo lo stesso," e ancora "...tutto un po' sotto tono, ma ci puoi stare," è tutt'ora fermamente convinto di avermi spronato e motivato allo studio per il raggiungimento dell'obiettivo. Andrea: "...grazie lo stesso."

Ringrazio la mia Relatrice, Prof.ssa Shaira Thobani, che stimo molto e che mi ha dato sin dall'inizio grandi stimoli, un costante supporto

e tanti spunti di riflessione per "ragionare" e mai imparare solo a memoria; un'eccellente insegnante, attenta, con un approccio all'insegnamento moderno, oltre che una giurista competente ed esperta.

Voglio inoltre ringraziare l'ufficio inclusione dell'Ateneo, nella persona del Prof. Gaetano Tieri ed anche la tutor del corso di laurea SCAMS, Dott.ssa Ersilia Crobe, entrambi sempre al mio fianco con concreto e costante supporto.

Ringrazio la Associazione Italiana Dislessia, che mi ha instradato e supportato all'inizio del percorso con preziosi consigli e informazioni.

In ultimo, ma certamente non meno importante, un pensiero va ai miei genitori che, nonostante la loro presenza e disponibilità, 30 anni fa sono stati spettatori, non senza una certa delusione, della mia scelta di non proseguire gli studi universitari; ebbene: "...scusate il ritardo!!!"

Roma, 21 Dicembre 2023

Fino di pubblicare nel marzo 2024

'RAGGIUNGERE UN IMPORTANTE RISULTATO

RIPAGA MOLTO PIÙ DI ENTUSIASMANTI MOTIVI PER NON AVERLO FATTO!

TTS
CENTRO STUDI SVILUPPO
RELAZIONI PER LA SICUREZZA