INTRODUZIONE

Nell'era in cui la gestione e la sicurezza dei dati rappresentano sfide sempre più complesse, la tutela della privacy emerge come un pilastro fondamentale, soprattutto all'interno delle aziende governative. La pubblica amministrazione, con il suo vasto patrimonio di dati sensibili, si trova al centro di una responsabilità cruciale: garantire la sicurezza e la conformità normativa nella gestione delle informazioni personali. In questo contesto, la figura del Data Protection Officer (DPO), figura inizialmente nata con la direttiva sulla tutela dei dati 95/46/CE e successivamente evolutasi (Regolamento europeo 679/2016), si configura come una figura chiave, incaricata di sovrintendere e garantire la conformità delle pratiche disposte dal regolamento. Nella pubblica amministrazione, la figura del DPO assume una rilevanza crescente, richiedendo competenze sofisticate, una profonda conoscenza delle leggi sulla privacy e la capacità di navigare tra gli intricati scenari della governance digitale. Questa tesi si propone di esplorare in dettaglio il ruolo del Data Protection Officer nella pubblica amministrazione, analizzandone le sfide, i successi e l'impatto sulla protezione dei dati personali. Attraverso un'indagine approfondita, ci si propone di fornire non solo una panoramica esaustiva delle responsabilità del DPO, ma anche di comprendere come questa figura chiave si sia evoluta nel tempo e contribuisca a plasmare una cultura di rispetto della privacy all'interno delle istituzioni governative, evidenziandone quelli che sono i requisiti e le caratteristiche. Le tematiche saranno analizzate nella tesi, in particolare il capitolo I sarà un'introduzione a quelle che sono le principali nozioni in tema di privacy e trattamento di dati personali e come si è evoluta la normativa della privacy nel tempo. Nel capitolo II si scenderà nel dettaglio della gestione dei dati personali analizzandone quelli che sono i principali rischi e cosa è previsto dal GDPR. Nel capitolo III verrà trattata la figura del Data

Protection Officer all'interno delle istituzioni comunitarie e nello specifico come questa figura è inserita in Italia nell'ambito della pubblica amministrazione, evidenziandone quelle che sono le criticità attualmente presenti. Si vedrà poi come il DPO opera in modo indipendente dalle istituzioni, in modo da poter garantirne l'autonomia e la massima imparzialità di fronte alle normative. Nel capitolo IV si andrà ad analizzare quelle che sono i requisiti e le caratteristiche specifiche della figura del Data Protection Officer, come viene nominato e le sue competenze. Si vedrà inoltre, un esempio di caso studio di data breach accaduto di recente in un ambito molto importante della PA, cioè quello sanitario.

CAPITOLO I – DIRITTO DELLA PRIVACY

1 Privacy: storia ed evoluzione

Il diritto alla privacy ha una storia molto lunga e complessa, che si è evoluta nel corso del tempo, influenzata da molteplici fattori culturali, sociali, filosofici e giuridici. A partire dall'antica Grecia, gli uomini avvertono il bisogno di costruirsi una casa come luogo fisico di appartenenza a una città per contribuire alla vita pubblica; infatti, «senza una casa un uomo non poteva partecipare agli affari della città, perché in essa non aveva un luogo che fosse propriamente suo»[1]Anche nella Roma antica ritroviamo un modello simile a quello ellenico, seppur con qualche differenza sostanziale; è noto, infatti, come nell'antica Roma, le vicissitudini degli imperatori e delle più grandi personalità di quel tempo, siano spesso state alla mercè di tutto il popolo; Andando avanti molti anni, più precisamente nel medioevo, si nota come la questione della riservatezza inizia a emergere grazie ai gruppi familiari, poiché "vita familiare viene intesa in senso conviviale, ove non vi era spazio per l'individualità"[2]. I primi cambiamenti, si ebbero, come possiamo

[1] S. Niger, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Cedam, Padova, 2006, cit., p. 2.
[2] F. Fabris, *Il diritto alla privacy tra passato, presente e futuro*, in *Tigor: rivista di scienze della comunicazione*, n.2 (luglio-dicembre), 2009, p. 95.

notare nell'opera di Lewis Mumford[3], con la nascita del senso di intimità, infatti, se prima la possibilità di isolarsi era privilegio di pochi, inizia in questo periodo a espandersi anche verso gli altri ceti sociali. Di lì in poi, si vedrà come la vita privata avrà dei cambiamenti verso la modernità, basta osservare i grandi proprietari terrieri, che disponevano infatti delle libertà personali dei propri sottoposti. In Europa, il concetto di privacy inizia a svilupparsi soltanto intorno alla fine del 1800, principalmente con tre correnti di pensiero, che elaborano il concetto di privacy in modi diversi tra loro. Mentre in Francia, l'orientamento è rivolto a quello che è la protezione dell'immagine e la tutela della vita privata, in Germania si sviluppa la corrente pandettistica dell'"Individualrecht". Lo "ius in sé ipsum", e cioè, il diritto di disporre di sé stesso e il diritto di impedire ai terzi di compiere atti volti a privarlo della potestà che gli spetta sul proprio corpo e sulle proprie facoltà psichiche[4], divenne un tema centrale nella riflessione di fine Ottocento, e contribuì a dare origine ai diritti della personalità. Grandi cambiamenti si ebbero, con il divulgarsi di un senso di diritto alla riservatezza soprattutto grazie agli sviluppi tecnologici, come la stampa e la fotografia. Infatti, solo recentemente se ne è iniziato a parlare sotto il profilo giuridico, e nello specifico grazie all'opera di due giuristi statunitensi, Samuel Warren e Louis Brandeis, con la loro opera sulla privacy intitolata "The Right to Privacy. The Implicit Made Explicit"[5]. L'opera, nata in seguito a vicende private del giurista Warren, ha infatti considerato la riservatezza, come un bene giuridico autonomo e tutelabile quale "diritto ad essere

[3] L. Mumford, *La cultura delle città*, trad. it. di E. e M. Labò, Einaudi editore, Milano, 1953, p. 29 <<il primo mutamento radicale destinato ad infrangere la forma della casa di abitazione medievale fu lo sviluppo del senso di intimità. Questo, infatti, significava la possibilità di appartarsi a volontà dalla vita e dalle occupazioni in comune coi propri associati. Intimità durante il sonno; intimità durante i pasti; intimità nel rituale religioso e sociale; e finalmente intimità nel pensiero.>>

[4] V. Campogrande, Ravà Adolfo, *I diritti sulla propria persona*, Editore F.lli Bocca 1896. Anche E. FERRI affronta il tema dei diritti sulla propria persona con la monografia L'omicidio-suicidio: responsabilità giuridica, Torino, 1884.

[5] S. D. Warren, L. D. Brandeis, *The Right to Privacy,* in *Harward Law Review*, IV, 1890.

lasciati soli"[6]. Grazie alla loro opera, vennero definiti dei confini quale disciplina autonoma, definendone le relative sanzioni e limiti giuridici.

In Europa, le prime sentenze si ebbero intorno agli anni '50, con oggetto principalmente vicende relative a fatti personali con riferimenti al diritto alla riservatezza. Per quanto riguarda i riferimenti normativi, si considerava quale ulteriore base a tutela della riservatezza l'art. 8 della Convenzione per la salvaguardia dei diritti dell'uomo, firmata nel 1950 e resa esecutiva in Italia nel 1955. Nel 1975, in Italia, fu il supremo collegio ad affermare l'esistenza del diritto alla riservatezza, Si giunge così al riconoscimento ed applicazione del diritto alla riservatezza come protezione dei dati personali in ambito comunitario con la Convenzione di Strasburgo e le conseguenti singole interpretazioni degli Stati nazionali. La questione della tutela dei dati personali, si pose principalmente con lo sviluppo di tecnologie sempre più all'avanguardia, che permettevano, di conservare una grande quantità di dati in spazi fino a prima inimmaginabili, con relative banche dati con informazioni personali, e con la grande facilità di trasmissione dei dati in maniera informatizzata, fu allora che il concetto di privacy assunse ancor più rilevanza. A semplificare le varie normative nazionali, fu la direttiva emanata dall'unione europea 95/46/CE relativa alla tutela delle persone fisiche, con riguardo ai dati personali, nonché alla libera circolazione dei dati, che istituì oltretutto la figura del Garante per la protezione dei dati personali, la Direttiva 97/66/CE, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, e la Direttiva 2002/58/CE, relativa al trattamento dei dati personali. In Italia, per rafforzare ulteriormente la tutela in materia di protezione di dati, fu introdotto il Codice della Privacy (D.lgs. 196/2003) che contribuì ulteriormente a dettare delle regole ben precise da seguire, e successivamente, con il regolamento UE 2016/679 (GDPR) si ebbe un quadro normativo a livello europeo con delle indicazioni specifiche da recepire per ogni

[6]M.Martorana, A.Tesoro, A.Barberisi , *GDPR: Guida pratica agli adempimenti privacy.* (par.1 cap.1), Wolters Kluwer Italia, Cedam 2018

stato membro. Si nota inoltre come il GDPR, entrato in vigore negli stati membri dell'unione dal 25 maggio 2018 porta con sé una novità: non si tratta più di una direttiva, ma bensì di un regolamento. Le direttive precedenti lasciavano agli stati membri un margine di operatività in relazione al recepimento negli ordinamenti nazionali (come abbiamo visto in Italia con la L. 675/1996, e successivamente, con il d.lgs. 196/2003, cd. Codice della privacy), mentre il regolamento, è un atto normativo immediatamente applicabile negli ordinamenti nazionali, e non lascia margine di discrezionalità agli stessi in ordine alla sua applicazione. Possiamo quindi desumere che lo scopo primo del regolamento europeo per la protezione dei dati personali, è stato senza dubbio quello di adeguare la disciplina sul trattamento dei dati personali alle moderne tecnologie, che, soprattutto in questa "era del digitale" che stiamo vivendo, sono divenute strumenti di controllo della vita di ognuno: l 'obiettivo è stato realizzato dando una normativa, decisamente più incisiva rispetto a quella del passato, proprio per garantire agli individui di far conoscere di sé solo quello che si vuole far conoscere.

2. La protezione dei dati personali

L'avvento dell'era digitale ha inaugurato un'epoca di trasformazione senza precedenti, ridefinendo radicalmente il nostro modo di vivere, lavorare e connetterci. Abbiamo visto che se in passato, il problema era limitato alla protezione di dati personali intesa come diritto alla riservatezza, nei tempi moderni, la questione della protezione dei dati assume un aspetto molto più espanso e importante. Infatti, il crescendo della società digitale, ha permeato ogni aspetto della nostra vita, dalla comunicazione all'intrattenimento, dal lavoro alla sfera personale. Questo scenario ha comportato un'incredibile espansione nella generazione dei dati personali, con milioni di individui che quotidianamente contribuiscono a un vasto ecosistema informativo. La protezione dei dati personali si basa su diversi principi: Il primo principio su cui voglio concentrarmi è la

consapevolezza e la trasparenza. Come cittadini, abbiamo il diritto di essere pienamente informati sulle modalità con cui le organizzazioni raccolgono, utilizzano e gestiscono i nostri dati personali. Questa consapevolezza è la base per garantire che le nostre informazioni siano trattate in modo equo e responsabile. Un secondo principio cardine è quello delle finalità limitate. I dati personali dovrebbero essere raccolti solo per scopi specifici e legittimi, evitando qualsiasi uso incompatibile con gli scopi originari. Questo assicura che le informazioni che condividiamo siano utilizzate in modo etico e in linea con le nostre aspettative. Il principio di minimizzazione dei dati sottolinea l'importanza di raccogliere solo le informazioni strettamente necessarie per raggiungere gli scopi dichiarati. Questo non solo protegge la nostra privacy, ma contribuisce anche a evitare la creazione di enormi depositi di dati superflui. È imperativo poi, che le aziende adottino misure rigorose per garantire la correttezza dei dati che trattano. Altro principio riguarda il tempo di conservazione dei dati personali, tali dati infatti, dovrebbero essere conservati solo per il periodo strettamente necessario per raggiungere gli scopi per i quali sono stati raccolti.

La responsabilità delle organizzazioni è un ulteriore principio chiave,esse sono responsabili della conformità alle normative sulla protezione dei dati e devono dimostrarla attraverso documentazione adeguata e pratiche di sicurezza.

Infine, ciascuno di noi ha il diritto di accedere alle proprie informazioni, richiederne la rettifica, chiederne la cancellazione e opporsi al trattamento. Questi diritti rappresentano la nostra difesa contro un uso improprio dei nostri dati personali.

2.1. Dato personale e trattamento

Il regolamento europeo, e dunque, la normativa nazionale di adeguamento al GDPR si applicano al trattamento dei dati personali delle persone fisiche. Ma esattamente cosa si intende per dato personale? Con il termine dato personale si intende "*qualsiasi informazione riguardante una persona fisica identificata o identificabile*"[7]. Da questa definizione si evince che i dati personali non sono solo quelli che a primo impatto potrebbero sembrare i più facili da reperire, come un semplice nome e cognome, infatti, il termine "*qualsiasi informazione*" comporta che tale concetto deve essere inteso in senso molto ampio, comprendendo anche quelli che sono i nuovi tipi di informazioni che con il contesto digitale vengono fortemente ampliati: basti pensare ad esempio ai dati che vengono condivisi sui social, a volte anche di proposito, relativi a posto di lavoro, titolo di istruzione, luogo di residenza, e ancora ai dati relativi all'ubicazione acquisiti tramite geolocalizzazione dello smartphone o agli identificativi online come indirizzi IP o dati elaborati tramite cookie. Il GDPR, inoltre, definisce come dati personali anche quelli genetici, biometrici, dati relativi alla salute fisica e mentale, comprese informazioni di natura sanitaria.

Un altro aspetto essenziale, riguarda le informazioni personali, che devono necessariamente coinvolgere individui fisici, escludendo quindi da questa classificazione tutte le informazioni relative a entità giuridiche. A proposito di persona fisica, è chiarito che la persona fisica deve essere identificabile o identificata, e la definizione prosegue specificando che "*si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua persona fisica, fisiologica, genetica, psichica, economica, culturale o sociale*"[8].

[7] Regolamento (UE) 2016/679, art.4 num. 1.
[8] Regolamento (UE) 2016/679, art.4 num.1.