ALMA MATER STUDIORUM - UNIVERSITA' DI BOLOGNA

SCUOLA DI SCIENZE

Corso di Laurea in Informatica per il Management

# Il nuovo Regolamento generale sulla protezione dei dati e il ruolo del *Data Protection Officer*

Relatore
Dott.ssa Matilde Ratti

Presentata da
Davide Scalinci

Sessione II
Anno Accademico 2018 / 2019

*Ad Albino e Nicola*

*e ai loro figli*

*Anna Rita ed Ernesto*

*per averli amati come non mai*

# Indice

# Capitolo 1

# Introduzione

La Carta dei diritti fondamentali dell'Unione europea, all'art. 8, garantisce ad ogni persona il diritto alla protezione dei dati di carattere personale che la riguardano ma il rapido avanzare delle tecnologie informatiche, degli strumenti di connessione tra le persone e l'assenza di una normativa uniforme per gli Stati europei ha messo in pericolo più volte questo fondamentale diritto.

Per offrire una tutela migliore, il legislatore europeo ha deciso di adottare un Regolamento che si applica a tutte le persone presenti nell'Unione europea e che per sua natura non necessita di alcun atto di recepimento da parte degli Stati membri: il Reg. UE 2016/679 (GDPR). Il Regolamento Generale sulla Protezione dei Dati è stato pubblicato nella Gazzetta Ufficiale dell'Unione europea il 4 Maggio 2016 e la sua applicazione decorreva dal 25 Maggio 2018.

Questo Regolamento fa in modo di focalizzare l'attenzione del titolare del trattamento e del responsabile del trattamento sull'importante questione della sicurezza riguardante la protezione dei dati e cerca, tramite l'assegnazione di specifici compiti, di creare un set di istruzioni da seguire per permettere all'interessato, i cui dati personali sono oggetto di trattamento, di veder rispettati i propri diritti. Sarà dunque l'approccio basato sul rischio, così come descritto nell'art. 32, a guidare le scelte del titolare del trattamento e del responsabile del trattamento, i quali dovranno decidere con accuratezza quali provvedimenti organizzativi e tecnologici impiegare per affrontare in modo proattivo i problemi di sicurezza.

Avere una visione di insieme dei rischi derivanti dal trattamento, dei vincoli giuridici, dei mezzi organizzativi e tecnologici da poter adottare, assicura un corretto approccio alle problematiche di sicurezza che affliggono i dati personali.

Per supportare nelle decisioni riguardanti la protezione dei dati personali tutti i soggetti coinvolti nel meccanismo di trattamento, il legislatore europeo all'art. 37 del Regolamento introduce una nuova figura chiamata responsabile della protezione dei dati (*Data Protection Officer*) che avrà un significativo peso nelle organizzazioni.

L'intento del presente elaborato è quello di fornire una panoramica riguardante il Regolamento Generale sulla Protezione dei Dati e descriverne alcuni aspetti che rappresentano una novità nello scenario giuridico.

# Capitolo 2

# Diritti dell'interessato

## – 2.1 –

# Vecchi e nuovi diritti dell'interessato

I diritti dell'interessato non sono qualcosa di nuovo e di mai affrontato prima dal legislatore, sono anzi l'oggetto primario che i vari strumenti legislativi in materia di protezione dei dati personali, emanati sinora dagli Stati membri, hanno cercato di tutelare; già diversi anni prima dell'ideazione del Regolamento i diritti dell'interessato erano esplicati all'interno della Direttiva 95/46/CE.

All'art. 12 della suddetta Direttiva viene descritto il diritto di ottenere dal responsabile del trattamento l'accesso ai propri dati «liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessive» e si fa inoltre cenno ai diritti di rettifica, cancellazione e congelamento dei dati mentre l'art. 14 è interamente dedicato al diritto di opposizione al trattamento.

Dal 1995 ad oggi è trascorso quasi un quarto di secolo e il passare del tempo ha portato con se un avanzamento tecnologico considerevole che ha prodotto molteplici benefici e innovazioni, ha visto la nascita di nuovi strumenti per diminuire la distanza tra le persone, i *social network*, l'*home banking* e i sistemi gestionali informatici come ad esempio quelli per le strutture ospedaliere che raccolgono i dati dei pazienti o anche i database presenti nei CRM (*Custom Relationship Management*) delle compagnie fornitrici di servizi.

Alla luce di quanto premesso, il contenuto del diritto di accesso nel nuovo Regolamento è stato arricchito e nuovi diritti come quello alla portabilità, prima non necessario per via della mancanza degli strumenti a cui è legato, sono stati aggiunti.

## – 2.2 –

# Il diritto di accesso

Se consapevole dei propri diritti, il soggetto interessato dal trattamento di dati personali ha nella sua "cassetta degli attrezzi" numerosi strumenti da poter utilizzare per controllare, e nel caso intervenire sui dati stessi, senza che questo richieda un grosso sforzo.

Per esercitare il controllo sui dati che lo riguardano, l'interessato deve necessariamente essere messo al corrente di alcune informazioni fondamentali, come l'identità e il recapito, per poter contattare il titolare del trattamento o il responsabile della protezione dei dati, in modo da ottenere la conferma o meno che sia effettivamente in corso un trattamento di dati personali, quali siano le finalità del trattamento attualmente in corso e se vi siano garanzie adeguate nel caso in cui i dati dovessero essere trasferiti in un Paese extra UE.

Vanno inoltre fornite all'interessato ulteriori informazioni riguardanti l'origine dei dati: nel caso in cui fossero state utilizzate varie fonti «dovrebbe essere fornita un'informazione di carattere generale»[1]; il periodo di conservazione dei dati o

[1] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 12; Considerando n. 61;

almeno quali sono i criteri utilizzati per determinare la durata; l'esistenza del diritto di proporre reclamo a un'autorità di controllo, di chiedere al titolare la rettifica, la cancellazione o limitazione del trattamento e anche di opporsi al trattamento in sé; l'esistenza di un processo decisionale automatizzato che potrebbe comprendere la profilazione e tutto ciò che riguarda un trattamento effettuato con una simile modalità.

Tutte queste informazioni rese disponibili, permettono all'interessato di mantenere il controllo sui propri dati e di essere in grado di verificare la liceità del trattamento e nel caso di porvi rimedio. Dall'altro lato il titolare del trattamento dovrebbe favorire il diritto di accesso il più possibile e, se la struttura organizzativa di cui fa parte lo permette, dovrebbe poter fornire un accesso remoto ad un sistema sicuro assimilabile ad una *sandbox*, magari utilizzando le ultime innovazioni in campo di virtualizzazione di sistemi, che permetta in maniera diretta la consultazione dei dati personali da parte del soggetto interessato il quale, facendone richiesta, può ottenerne una copia gratuita.

Se al titolare del trattamento fossero richieste ulteriori copie dei dati, potrebbe decidere di addebitare delle spese ragionevoli al richiedente per l'espletamento della pratica. Questa procedura non lede il diritto di accesso, ma bensì ha il duplice beneficio di non indisporre il titolare a fornire le copie e limita l'abuso di richieste da parte dell'interessato. Per fare un parallelo con il mondo informatico, la possibilità da parte del titolare di chiedere una ragionevole somma può essere vista come un modo per proteggersi da un attacco DoS (*Denial of Service*) da parte dell'interessato che per qualche ragione decide di "inondare" di richieste, e quindi provocare disagio, al titolare del trattamento.

Non va inoltre dimenticato che nell'ottenere la copia dei dati, i diritti e le libertà altrui non devono in alcun modo essere lese; infatti qualora i dati personali

dell'interessato dovessero trovarsi, ad esempio, in dei moduli insieme ai dati personali di qualche altro soggetto, quest'ultimi dovrebbero essere prima oscurati. L'unico caso in cui è concesso accedere ai dati di soggetti terzi, si configura quando questi sono talmente tanto aggrovigliati ai dati dell'interessato che precluderne l'accesso renderebbe incomprensibili le informazioni necessarie all'interessato.

Infine il titolare del trattamento ha il compito di adempiere alla richiesta al massimo entro un mese, nonostante possa beneficiare di una proroga dopo aver informato l'interessato. Se la richiesta è effettuata mediante mezzi elettronici e l'interessato non specifica una modalità differente, il titolare è tenuto a fornire le informazioni in un formato elettronico di uso comune.

## – 2.3 –

# Il diritto alla portabilità

Nel momento in cui dati personali sono raccolti, il titolare, per garantirne un corretto e trasparente trattamento, fornisce all'interessato diverse informazioni, tra cui l'esistenza del diritto dell'interessato a richiederne la portabilità.

Come detto in precedenza, il diritto alla portabilità dei dati entra a far parte dei diritti dell'interessato come una delle novità del Regolamento rispetto alla Direttiva 95/46/CE. Questo si configura come un ampliamento o rafforzamento del diritto di accesso. Infatti, esercitandolo, una copia dei dati personali viene ottenuta dall'interessato ed è necessario far notare che, anche attraverso il diritto di accesso, l'interessato può procurarsi (almeno una) copia dei dati stessi.

Quando si parla di rafforzamento del diritto di accesso si intende, per estensione, un aumento del potere di controllo da parte dell'interessato sui propri dati e rappresenta uno dei vantaggi che il diritto alla portabilità genera. Un altro vantaggio consiste nell'aumento della concorrenza tra fornitori di servizi, nonché nel necessario sviluppo di tecnologie compatibili tra loro, per il trasferimento e l'interpretazione dei dati oggetto di portabilità, adoperate dai diversi soggetti che sono, oppure diventeranno, titolari del trattamento di quei dati.

La portabilità dei dati, inoltre, sposta l'ago della bilancia del potere contrattuale un po' più al centro rispetto a quanto non fosse prima. Riequilibra cioè quel rapporto instauratosi tra titolare del trattamento e interessato a favore di quest'ultimo[2], che può facilmente ottenere il trasferimento dei propri dati personali verso un altro titolare.

Tramite il diritto alla portabilità dunque, l'interessato ha la possibilità di ottenere copia dei propri dati personali per uso privato in un formato strutturato, di uso comune e leggibile da dispositivo automatico, ad esempio richiedendo la propria rubrica di indirizzi email per poterla poi utilizzare per scopi privati, e può ottenere il trasferimento diretto degli stessi dati da un titolare ad un altro[3].

Il diritto alla portabilità, come espresso nell'art. 20 del Regolamento, non è applicabile a tutti i trattamenti di dati come nel caso del suo "fratello maggiore" il diritto di accesso. Diventa esercitabile quando ricorrono almeno due condizioni, la prima delle quali è che siano utilizzati mezzi automatizzati per effettuare il trattamento. Questo significa che, qualora dovessero verificarsi le altre condizioni ma il trattamento dei dati dovesse essere svolto senza l'ausilio di mezzi automatizzati, il diritto alla portabilità potrebbe non essere garantito. La seconda condizione può consistere alternativamente in uno di questi requisiti[4]: l'interessato deve aver espresso il consenso al trattamento per una o più specifiche finalità;

---

[2] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sul diritto alla portabilità dei dati; Pagina 4; «Il diritto in questione offre anche la possibilità di "riequilibrare" il rapporto fra interessati e titolari del trattamento tramite l'affermazione dei diritti e del controllo spettanti agli interessati in rapporto ai dati personali che li riguardano»

[3] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 45; Articolo 20 paragrafo 1; «L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento cui li ha forniti […]»

[4] Nell'art. 20 paragrafo 1, lettera a) viene fatto riferimento all'art. 6, paragrafo 1, lettere a) e b) e all'art. 9, paragrafo 2, lettera a)

oppure aver prestato il consenso esplicito al trattamento dei propri dati sensibili[5] riguardanti l'origine razziale o etnica, opinioni politiche, dati genetici, biometrici, relativi alla salute, alla vita e all'orientamento sessuale; o, infine, aver prestato il consenso come una delle parti all'interno di un contratto.

Esattamente come per il diritto all'accesso, anche l'esercizio del diritto alla portabilità non deve in nessun modo ledere le libertà e i diritti altrui e, inoltre, non può costituire una esimente nell'adempimento degli altri diritti dell'interessato da parte del titolare. In altre parole, una eventuale futura richiesta di portabilità non può essere utilizzata dal titolare come motivazione per svicolare dalle responsabilità derivanti dal dover osservare un qualsiasi altro diritto dell'interessato. Per questa ragione, il titolare del trattamento non può, ad esempio, rifiutarsi di cancellare i dati personali dell'interessato che ne faccia richiesta, soltanto perché in un momento successivo quest'ultimo potrebbe volerne effettuare la portabilità verso un altro titolare.

Uno degli esempi più calzanti è rappresentato dalla portabilità del proprio numero di telefono[6]; infatti questa pratica garantisce all'utente, quindi ad un soggetto che ha sottoscritto un contratto commerciale i cui dati sensibili sono trattati con mezzi automatizzati, di mantenere il proprio numero telefonico ovvero di trasferire i propri dati ad un'altra compagnia telefonica, che avrà tutti i mezzi necessari per riceverli direttamente dalla compagnia precedente ed iniziarne così il trattamento.

---

[5] Il Garante per la protezione dei dati personali chiarisce in un documento cosa si intenda per dati personali e specifica quali di questi sono dati "sensibili" «cioè quelli che rivelano l'origine razziale od etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'appartenenza sindacale, relativi alla salute o alla vita sessuale»

[6] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 220; «[…] La portabilità del numero consente agli utenti di conservare il proprio numero telefonico all'atto di cambiamento del gestore del servizio […]»

I benefici generati dal diritto alla portabilità non riguardano soltanto l'interessato, ma anche il titolare del trattamento (in questo caso le compagnie telefoniche), perché la ricerca e la conseguente creazione e utilizzo di tecnologie compatibili o addirittura l'ideazione di uno standard per far si che i dati siano facilmente trasmissibili, leggibili e usabili, rappresentano non solo un avanzamento tecnologico, ma anche un'arma in più da poter sfruttare per poter aumentare il proprio portafoglio clienti a scapito delle compagnie avversarie.

Il Gruppo di lavoro articolo 29 (*Article 29 Data Protection Working Party)* attraverso le sue Linee Guida si esprime sul diritto alla portabilità per renderne l'applicazione più chiara e semplice. Secondo le Linee Guida, quando un titolare riceve la richiesta di portabilità dei dati personali, deve fare in modo di fornire quei dati che possano soddisfare il fine ultimo della richiesta, così che siano rilevanti per l'interessato in caso di utilizzo per fini privati o favoriscano il trattamento da parte di un altro titolare. Se prendiamo come esempio un *social network*, il titolare non dovrebbe fornire solo i dati che l'interessato ha inserito nel *form* per la registrazione al servizio, ma anche tutti quei dati che, proprio dall'utilizzo da parte dell'utente del servizio stesso, sono stati creati e raccolti.

Un altro punto su cui fanno chiarezza le Linee Guida è la modalità con cui il titolare deve soddisfare la richiesta di portabilità, e cerca di spingere per l'adozione e l'utilizzo di forme automatiche, come la funzione di *download* diretto attraverso interfacce *software* facilmente raggiungibili.

Così come il titolare non può in alcun modo trattenere i dati per una eventuale futura richiesta di portabilità, alla stessa maniera non ha l'obbligo di conservarli se

lo scopo per cui ha effettuato la raccolta e il trattamento è stato raggiunto[7]. Quando viene a manifestarsi il caso in cui il periodo di conservazione dei dati ha ultimato la sua utilità, e quindi l'obiettivo per cui i dati personali erano stati raccolti è stato conseguito, il titolare deve informare l'interessato che a breve effettuerà la cancellazione, così che quest'ultimo possa richiedere la portabilità e non perdere tutte quelle informazioni che potrebbero essere ritenute rilevanti e quindi conservate.

Una volta che il titolare del trattamento ha risposto alla richiesta di portabilità, non è responsabile per il trattamento che l'interessato (o una società ricevente i dati) effettua; infatti è il soggetto che riceve i dati a diventare titolare del trattamento e ha l'obbligo, dunque, di trattare i dati solo per le finalità per cui li ha ricevuti[8].

Infine, nel caso in cui il titolare effettui il trattamento per motivi di pubblico interesse, il diritto alla portabilità dei dati da parte dell'interessato non è esercitabile.

[7] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sul diritto alla portabilità dei dati; Pagina 7, «[…] non impone alcun obbligo ulteriore di conservazione dei dati personali al solo scopo di adempiere a una potenziale richiesta di portabilità»

[8] Nel Regolamento questo spostamento delle responsabilità rientra nella definizione di *Controllership*

# Capitolo 3

# Nuovo approccio al Regolamento basato sul rischio

## – 3.1 –

# Privacy by design e privacy by default

Il Regolamento per cercare di proteggere il più possibile i dati personali degli interessati, introduce tra i suoi articoli quello che obbliga il titolare del trattamento alla protezione dei dati sin dalla progettazione e alla protezione per impostazione predefinita.

I principi di *privacy by design* e *privacy by default* raffigurano un innovativo approccio alla protezione dei dati anche dal punto di vista concettuale. Fanno si che l'attenzione alla tutela dei dati nasca ancora prima che questi vengano raccolti, infatti, se un'impresa volesse avviare un nuovo progetto che includa, tra le altre cose, la raccolta di dati personali dovrebbe fin da subito prevedere quali strumenti adoperare per evitare un illecito trattamento.

Le norme presenti all'interno del Regolamento sono guidate da un criterio di valutazione del rischio, attraverso cui si determina la misura di responsabilità del titolare, tenendo conto di vari fattori come la natura, l'oggetto, il contesto e le finalità del trattamento.

Il concetto di *privacy by design* prevede che già dalla fase di progettazione, la protezione dei dati sia integrata nel ciclo di vita della tecnologia, in modo tale da poter prevenire il verificarsi dei rischi e permettere, al titolare del trattamento, di attuare interventi organizzativi e tecnici come la pseudonimizzazione per soddisfare efficacemente i principi di protezione dei dati[9].

La pseudonimizzazione, come riportato nell'art. 4 del Regolamento, rappresenta la metodologia attraverso la quale «i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive». Le informazioni aggiuntive a cui fa riferimento la definizione devono necessariamente essere conservate separatamente e non devono poter essere ricondotte ad una persona fisica. Le tecniche di pseudonimizzazione portano il titolare del trattamento all'individuazione di quali variabili sono degli identificatori diretti, come può esserlo il codice fiscale, quali variabili sono degli identificatori indiretti, come la data di nascita, e quali invece possono essere ignorate durante il processo. Se si utilizza un *database* relazionale per la memorizzazione dei dati, dopo aver individuato le variabili, un modo per attuare la pseudonimizzazione è, ad esempio, quello di passare alla fase di sostituzione, che scambia il contenuto di una colonna presente in una tabella del DB con il contenuto di un'altra colonna di un'altra tabella contenente dati simili ma immaginari. In questa maniera il dato mantiene la sua consistenza, per via delle regole presenti nel *database,* ma non è più riconducibile alla singola persona fisica.

L'art. 25, inoltre, porta il titolare del trattamento a garantire che, per impostazione predefinita (*privacy by default*), siano trattati soltanto i dati personali necessari alle finalità del trattamento, per un periodo di tempo proporzionato al conseguimento dello scopo e che la quantità di dati raccolti non sia eccessiva, ma rappresenti la

[9] Colombo M.; Regolamento privacy UE 2016/679: Principi generali e Ruolo del Data Protection Officer; Pagina 72

quantità minima indispensabile per perseguire le finalità, in questo caso il Regolamento indica tale pratica con il termine minimizzazione.

Ogni titolare del trattamento, seguendo un meccanismo di certificazione[10], può comprovare la propria adesione a questi principi. In ogni caso, prima della progettazione e della messa in opera del sistema per il trattamento automatizzato dei dati, il titolare del trattamento deve consultare il *Data Protection Officer* (se è stato designato) per essere sicuro di muoversi nella giusta direzione. Analizzare dunque i rischi prima della creazione del servizio (o prodotto) che infine poi darà luogo al trattamento, costituisce uno dei migliori approcci per l'attenuazione degli stessi.

[10] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 58-59; Articolo 42 paragrafi 1 e 3; «Gli Stati membri […] incoraggiano […] l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento» «La certificazione è volontaria e accessibile tramite una procedura trasparente»

## – 3.2 –

# Valutazione di impatto

Il Regolamento obbliga le aziende ad essere *risk driven*, ovvero a far sì che il fattore fondamentale che influenza le loro scelte durante la creazione di servizi (o prodotti) che comportano il trattamento di dati, sia il rischio.

Il rischio è caratterizzato dalla probabilità che l'attività dannosa ad esso relativa si verifichi, le cause sono da ricercare nelle vulnerabilità del sistema utilizzato, e dalla rilevanza degli effetti che il rischio stesso può provocare, le cui motivazioni vanno invece ricercate nella quantità di dati raccolti, nella loro tipologia e nel numero di soggetti interessati[11]. Nel caso in cui si dovesse riscontrare che l'utilizzo delle nuove tecnologie che il titolare vuole adoperare possa comportare un livello di rischio elevato per i diritti e le libertà delle persone fisiche, è necessario effettuare una valutazione di impatto dei trattamenti, per decidere quali sono le contromisure da adottare in modo da contrastare i fattori di rischio e farli diminuire. Un insieme di trattamenti che presentano rischi simili, possono essere esaminati attraverso la

[11] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 302-303

stessa valutazione di impatto[12]; si adotteranno così soluzioni simili per problemi simili e al contempo si potranno anche contenere i costi derivanti dalla gestione del rischio in quanto non sarà necessario effettuare ulteriori valutazioni.

Il terzo paragrafo dell'art. 35 del Regolamento dispone che la valutazione di impatto è obbligatoria nei casi in cui si verifichi, tramite trattamento automatizzato, come può esserlo la profilazione, un'analisi dettagliata di informazioni relative a persone fisiche che vengono adoperate per assumere decisioni; o anche il trattamento su larga scala di categorie particolari di dati, come ad esempio quelli sensibili, oppure la sorveglianza sistematica di una zona accessibile al pubblico.

Il Regolamento specifica poi quali sono le caratteristiche necessarie a formare la valutazione di impatto. Infatti la documentazione deve contenere almeno la descrizione dei trattamenti previsti e delle finalità degli stessi, un'analisi riguardante la necessità e la proporzionalità dei trattamenti rispetto alle finalità per cui sono effettuati, la valutazione dei rischi per i diritti e le libertà degli interessati che rappresenta la sezione fondamentale, insieme a quella relativa alle contromisure ideate per contrastare i rischi, illustrando le garanzie e i meccanismi di sicurezza per la protezione dei dati personali[13].

All'interno della valutazione di impatto vengono analizzati anche gli aspetti più tecnici come l'anonimizzazione o la pseudonimizzazione, la realizzazione, l'organizzazione e l'utilizzo di *database,* il tempo di conservazione dei dati e la scelta o meno di coinvolgere i soggetti interessati. La presenza di particolari tecnici è uno dei motivi che ha portato il legislatore europeo a far sì che il titolare del trattamento

---

[12] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 53; Articolo 35 paragrafo 1; «[…] Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi»

[13] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 54; Articolo 35 paragrafo 7

effettui la valutazione di impatto consultando il *Data Protection Officer*, il quale fornisce un proprio giudizio riguardante la valutazione e ne sorveglia l'attuazione[14]. Il parere che il DPO fornisce riguarderà quale metodo dovrà essere seguito per effettuare la valutazione, se vi siano gli estremi per garantirne un corretto svolgimento in *outsourcing* oppure se sia preferibile sviluppare tale attività internamente. Una volta verificato che la valutazione di impatto è stata validamente eseguita, il *Data Protection Officer* redige le proprie conclusioni che indicano quali misure applicare e se sia possibile procedere con il trattamento dei dati personali o meno. Ovviamente nonostante il parere del DPO sia fortemente rilevante, rimane pur sempre un parere e non è dunque vincolante ai fini della decisione finale sull'effettuare o meno il trattamento, infatti, nel caso in cui il titolare o il responsabile optassero per il respingimento delle opinioni fornite dal *Data Protection Officer,* questi ne avrebbero la completa autonomia ma dovrebbero necessariamente documentare i motivi che hanno portato a tale decisione[15].

Infine, nel caso in cui il titolare non dovesse riuscire a trovare, neanche con l'ausilio del DPO, contromisure per la mitigazione o eliminazione del rischio palesatesi durante l'attività di valutazione, servirà contattare l'autorità di controllo che indicherà quali misure implementare oppure vieterà il trattamento.

---

[14] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettera c)

[15] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 363; «[…] I pareri espressi dal DPO, pertanto, assumono un valore di assoluto rilievo, seppur non vincolante, tanto che qualora il titolare o il responsabile intendano discostarsi dalle indicazioni espresse, saranno tenuti a documentare le motivazioni poste a fondamento della propria decisione»

## – 3.3 –

# Consultazione preventiva

Il considerando n. 89 del Regolamento fa notare che già nella Direttiva 95/46/CE era presente l'obbligo di notificare il trattamento dei dati personali alle autorità di controllo[16], ma anche che tale notifica non ha sempre assolto lo scopo di migliorare la protezione dei dati personali, nonostante comportasse dei costi da sostenere, e si è pertanto reso necessario, in un'ottica di maggior tutela, sostituire l'obbligo indiscriminato di notifica[17] con procedure e meccanismi più incentrati su quei trattamenti che potrebbero rappresentare un rischio elevato per le persone fisiche, soprattutto se tali trattamenti implicano l'utilizzo di nuove tecnologie. Pertanto la consultazione dell'autorità di controllo da parte del titolare non rappresenta più un obbligo ma una eventualità.

Quando la valutazione di impatto evidenzia che in assenza dell'adozione di misure da parte del titolare, il trattamento presenterebbe alti rischi, il titolare prima di

---

[16] Parlamento europeo, Consiglio dell'Unione europea; Direttiva 95/46/CE; Pagina 43-44; Articolo 18 paragrafo 1; «Gli Stati membri prevedono un obbligo di notificazione a carico del responsabile del trattamento, od eventualmente di un suo rappresentante, presso l'autorità di controllo […] prima di procedere alla realizzazione di un trattamento, o di un insieme di trattamenti […]»

[17] Il Regolamento 2016/679 abolisce l'art. 37 del Codice in materia di protezione dei dati personali D. Lgs. 196/2003

procedere al trattamento consulta l'autorità di controllo[18] fornendo, oltre alla valutazione di impatto, un dettaglio delle proprie responsabilità e di tutti coloro che concorrono alla titolarità del trattamento, compreso il responsabile, indica le finalità e i mezzi del trattamento, le garanzie e le misure applicate per proteggere i diritti degli interessati e fornisce anche i dati di contatto del *Data Protection Officer* e qualunque altra informazione venga richiesta dall'autorità di controllo.

L'autorità di controllo vaglierà la richiesta del titolare del trattamento e ne fornirà un riscontro scritto entro otto settimane, ma se l'analisi del trattamento, data la complessità, dovesse richiedere ulteriore tempo, l'autorità potrà beneficiare di altre sei settimane informando il titolare di questa necessità entro un mese dal ricevimento della richiesta. Il titolare del trattamento otterrà, come risposta alla propria richiesta, un ammonimento riguardante le violazioni del Regolamento e l'obbligo di adeguarsi allo stesso adottando determinate misure rispettando un certo periodo di tempo[19]. Ovviamente c'è da considerare il fatto che il titolare del trattamento dovrebbe aver già provveduto ad attenuare il rischio tramite l'adozione di «misure opportune in termini di tecnologia disponibile e costi di attuazione»[20], pertanto è anche possibile che l'autorità di controllo, invece di fornire dei correttivi, decida di negare il trattamento dei dati personali.

Questo modello per la gestione del rischio introdotto dal Regolamento, cerca di essere una soluzione intermedia tra la necessità di maggiore sicurezza, che potrebbe essere assicurata dall'effettuare una richiesta di verifica preventiva all'autorità di

---

[18] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 54; Articolo 36 paragrafo 1; « Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato […]»

[19] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 69-70; Articolo 58 paragrafo 2 lettere b) e d)

[20] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 16; Considerando n. 84

controllo, che però comporterebbe dei costi di gestione molto alti e rallentamenti nei processi di attuazione, e la pratica della autovalutazione controbilanciata dalle verifiche a campione effettuate dall'autorità di controllo, che avrebbe dei costi inferiori, ma lascerebbe troppo spazio a possibili errori, che si tradurrebbero facilmente in delle falle di sicurezza che conseguentemente potrebbero diventare violazioni dei diritti degli interessati[21].

[21] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 319; «[…] l'impianto dell'art. 36 genera un modello similautorizzatorio, unito però ad un filtro preventivo basato sull'auto-valutazione […]»

# Capitolo 4

# Il Data Protection Officer

## – 4.1 –

# Una (nuova) importante figura

I dati personali riguardano aspetti della vita privata delle persone, però non si tratta soltanto di un insieme di dati a sé stante ma bensì rappresentano informazioni, che utilizzate in modo inappropriato, possono produrre dei danni rilevanti. La pericolosità di una errata gestione dei dati è nota al legislatore europeo, così come è nota la mancanza di una legislatura comune a tutti gli Stati membri che possa garantire un buon livello di protezione. Se a questo si aggiunge poi, il sempre maggiore utilizzo da parte degli utenti di servizi digitali, che a volte per scarsa attenzione e a volte per scarsa chiarezza, prestano il consenso accettando le "condizioni di utilizzo" senza porsi troppe domande, si inizia ad intuire quanto il Regolamento fosse un passo necessario da compiere.

La complessità dei mezzi utilizzati per il trattamento e la continua evoluzione che li coinvolge ha portato il legislatore alla decisione di affiancare al titolare del trattamento e al responsabile del trattamento una figura con conoscenze specialistiche, non solo in ambito legale ma anche in ambito tecnico[22].

[22] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 18; Considerando n. 97; «[…] il titolare del trattamento o il responsabile del trattamento dovrebbe essere assistito da una persona che abbia una conoscenza specialistica della normativa e delle pratiche in materia di protezione dei dati nel controllo del rispetto a livello interno del presente regolamento. […]»

Il *Data Protection Officer* come supporto al titolare e al responsabile del trattamento non è una novità assoluta infatti «in alcuni Paesi europei [invece] la figura del DPO risulta essere già disciplinata dalla legislazione interna, tanto che, al ricorrere di determinate condizioni, essa viene prevista addirittura come obbligatoria, come ad esempio avviene in Germania, Austria e Repubblica Ceca»[23]. In Italia invece, prima dell'arrivo del Regolamento, soltanto poche imprese ed enti pubblici hanno deciso di affidarsi ad una figura che si occupasse della protezione dei dati. Questo denota una bassa attenzione al problema della tutela dei dati personali ed aumenta ancora di più la ragion d'essere del Regolamento.

All'interno dell'organigramma aziendale, il *Data Protection Officer*, deve essere considerato come un qualunque altro manager dell'azienda che svolge le proprie funzioni di controllo e consulenza in completa indipendenza. Il titolare del trattamento e il responsabile del trattamento sono i referenti diretti del DPO e sono tenuti a garantire che quest'ultimo durante l'assolvimento dei propri compiti non sia destinatario di qualche particolare indicazione in materia di protezione dei dati personali e su tutto ciò che riguarda la sua funzione di controllore[24]. Se poi dovesse aver fornito un parere, per far si che le decisioni del titolare del trattamento siano aderenti al Regolamento, ma venisse ignorato, dovrebbe poter manifestare il proprio disaccordo con tali decisioni. A tal proposito il titolare del trattamento e il responsabile del trattamento devono assicurarsi che il DPO non possa subire alcuna penalizzazione per lo svolgimento dei propri compiti né tanto meno possa

[23] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 333

[24] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 38 paragrafo 3; «Il titolare del trattamento e il responsabile del trattamento si assicurano che il responsabile della protezione dei dati non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti. […] Il responsabile della protezione dei dati riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento.»

essere rimosso dall'incarico[25]. Tuttavia, nel caso si verificasse una violazione del Regolamento e questa portasse ad un risarcimento in favore di soggetti terzi, nonostante la responsabilità di rispettare il Regolamento[26] e di corrispondere il risarcimento[27] sia di competenza del titolare del trattamento, il *Data Protection Officer* potrebbe dover risarcire il titolare se venisse provato che gli inadempimenti alla normativa sono dipesi da colpa o dolo dello stesso[28].

L'indipendenza del DPO è collegata al ruolo che egli ricopre nell'organizzazione. Oltre ad essere incaricato come responsabile della protezione dei dati, può svolgere ulteriori funzioni e ricoprire altri ruoli purché nessuno di questi preveda la definizione delle finalità del trattamento dei dati personali altrimenti si troverebbe in una posizione di conflitto di interessi[29]. Per evitare simili situazioni sarebbe pertanto consigliato, come buona pratica, che il titolare del trattamento, conoscendo bene la propria organizzazione, descriva tramite un documento interno quali posizioni possono essere ricoperte unitamente a quella di DPO.

---

[25] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 38 paragrafo 3; «[…] Il responsabile della protezione dei dati non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti. […]»

[26] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 36; Articolo 5 paragrafo 2; «Il titolare del trattamento è competente per il rispetto del paragrafo 1 [principi applicabili al trattamento di dati personali] e in grado di comprovarlo («responsabilizzazione»)»

[27] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 81; Articolo 82 paragrafo 1; «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»

[28] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 355; Nota n. 37; «[…] qualora gli inadempimenti alla normativa siano dipesi da colpa o dolo del DPO, essi potranno costituire oggetto di pretese risarcitorie «interne» da parte del titolare o del responsabile. […]»

[29] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 38 paragrafo 6; «Il responsabile della protezione dei dati può svolgere altri compiti e funzioni. Il titolare del trattamento o il responsabile del trattamento si assicura che tali compiti e funzioni non diano adito a un conflitto di interessi»

Affinchè i compiti previsti da Regolamento siano svolti correttamente dal DPO, il titolare del trattamento e il responsabile del trattamento hanno l'obbligo di supportarlo economicamente fornendogli le risorse appropriate per lo svolgimento delle attività legate alla protezione dei dati personali[30]. Ovviamente l'esborso economico deve essere proporzionato alla tipologia del trattamento che si vuole eseguire, pertanto è ragionevole ipotizzare che trattamenti più complessi richiedano risorse economiche più cospicue per garantire la giusta protezione dei dati personali.

Inoltre, le risorse economiche messe a disposizione del DPO devono essere sufficienti a coprire anche i costi derivanti dal mantenimento del livello specialistico della sua conoscenza, ovvero le spese per la partecipazione ai corsi di formazione, convegni, laboratori etc., in modo che possa sempre rimanere aggiornato sulle novità riguardanti la protezione dei dati personali.

Dato il particolare ruolo che il DPO ricopre all'interno dell'organizzazione, è molto importante che sia facilmente raggiungibile, soprattutto in casi di emergenza come può esserlo un *data breach*. Le Linee Guida del Gruppo di lavoro articolo 29 (*Article 29 Data Protection Working Party*) fanno chiarezza sulla questione dichiarando che i dati del DPO «dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD [DPO] stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il RPD[DPO] pubblicato sul sito del titolare/responsabile

[30] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 38 paragrafo 2; «Il titolare e del trattamento e il responsabile del trattamento sostengono il responsabile della protezione dei dati nell'esecuzione dei compiti di cui all'articolo 39 fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica»

del trattamento»[31]. Si tratta dunque di informazioni che rendono effettivamente reperibile il DPO in tempi molto brevi e forniscono un contatto diretto sia all'interno dell'organizzazione, sia all'esterno, ovvero ai soggetti interessati dal trattamento e alle Autorità di controllo.

Va poi ricordato che la figura del DPO può essere ricoperta non solo da una persona fisica, ma anche da una persona giuridica esterna all'organizzazione[32], purché il titolare del trattamento sia in possesso delle informazioni di contatto di una precisa persona fisica come riferimento.

[31] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 16 - 17

[32] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 55; Articolo 37 paragrafo 6; «Il responsabile della protezione dei dati può essere un dipendente del titolare del trattamento o del responsabile del trattamento oppure assolvere i suoi compiti in base a un contratto di servizi»

## – 4.2 –

# Requisiti e funzioni

Il Regolamento non elenca precisamente quali siano le caratteristiche professionali che un titolare del trattamento dovrebbe ricercare nella figura del DPO, ma mette in evidenza la necessità che abbia una approfondita conoscenza del Regolamento stesso e che, a seconda della tipologia dei trattamenti e della conseguente forma di protezione richiesta, abbia una conoscenza specialistica della materia trattata. Il *Data Protection Officer* deve dunque essere in grado di svolgere i propri compiti come riuscire a soddisfare le richieste di tutela dei dati provenienti dal titolare del trattamento, e quindi avere una conoscenza specifica del settore di attività in cui andrà ad operare.

Nella valutazione per la scelta di un DPO, il titolare del trattamento dovrebbe tener conto dell'organizzazione della propria azienda (o ente), dei possibili problemi che potrebbero svilupparsi e confrontare il tutto con l'esperienza maturata e messa a disposizione dal DPO.

Se il *core business* dell'organizzazione del titolare non è direttamente legato al trattamento dei dati personali, l'esperienza del DPO può limitarsi a tre anni, se al contrario rappresenta la mansione principale, allora l'esperienza richiesta dovrebbe essere di un minimo di sette anni.

Le competenze professionali di cui il DPO dispone devono sempre rimanere di alto livello e, pertanto, il Regolamento afferma che il titolare deve supportare economicamente la crescita professionale del DPO, ma nulla vieta che quest'ultimo faccia fronte da solo a tali spese.

Ovviamente, tra i requisiti utili ad un DPO fanno sempre una buona impressione capacità come la gestione di situazioni difficili, l'organizzazione, la discrezione e l'integrità morale. Il ruolo del DPO all'interno dell'organizzazione è di assoluta importanza, infatti non si occupa soltanto di controllare che i dati personali siano trattati nel pieno rispetto del Regolamento[33], ma svolge anche la funzione di consulente per tutti coloro che nell'organizzazione siano coinvolti nel trattamento dei dati personali[34]. Inoltre svolge importanti funzioni anche verso l'esterno dell'organizzazione, cooperando con l'Autorità di controllo e comunicando con i soggetti interessati dal trattamento[35]. La sua figura, dunque, non solo è importante, ma è anche centrale, viene coinvolto di fatto in tutte le fasi del trattamento, anche prima che questo avvenga, come nel caso della valutazione di impatto[36]. Il DPO ha così la funzione di lavorare insieme al titolare e al responsabile del trattamento per «dare attuazione agli elementi essenziali del regolamento quali i principi

---

33 Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettera b); «sorvegliare l'osservanza del presente regolamento, di altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali […]»

34 Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettera a); «informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento nonché da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati»

35 Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettere d) ed e); «cooperare con l'autorità di controllo; e», «fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione»

36 Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettera c); «fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35»

fondamentali del trattamento (Capo II), i diritti degli interessati (Capo III), la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita, i registri delle attività di trattamento (art. 30), la sicurezza dei trattamenti (art. 32), nonché la notifica di una violazione dei dati personali all'Autorità di controllo e la comunicazione di una violazione dei dati personali all'interessato (artt. 33 e 34), oltre a prestare la propria consulenza in caso di valutazione di impatto (art. 35), rapportandosi con l'Autorità di controllo (art.36)»[37].

Date le capacità professionali possedute dal DPO, sia in ambito giuridico che informatico, il compito di sorvegliare che le operazioni di trattamento siano svolte nel rispetto del Regolamento non si limita solo a tale attività ma viene esteso anche al controllo dell'attribuzione delle responsabilità e del processo di formazione del personale[38]. In questo modo è possibile assicurarsi che tutti coloro che si occupano del trattamento siano a conoscenza dei limiti imposti e vengano sensibilizzati sull'importanza della sicurezza dei dati personali.

L'art. 38 paragrafo 4 porta poi il DPO ad affiancarsi al titolare, dovendo comunicare efficacemente con i soggetti interessati dal trattamento per l'esercizio dei propri diritti e per tutto ciò che riguarda il trattamento dei loro dati personali.

Considerato l'elevato numero di informazioni a cui il DPO ha accesso, siano esse inerenti all'organizzazione o agli interessati, è tenuto alla massima riservatezza, ad eccezione della possibilità di consultare l'Autorità di controllo.

---

[37] AA. VV.; Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali; Pagina 348;

[38] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 56; Articolo 39 paragrafo 1 lettera b); «[sorvegliare l'osservanza del Regolamento e di altre disposizioni] […] compresi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale che partecipa ai trattamenti e alle connesse attività di controllo»

Uno dei possibili compiti aggiuntivi che potrebbe essere assegnato al *Data Protection Officer* dal titolare è quello di tenere sotto la propria responsabilità il registro delle operazioni di trattamento. Si tratta di un documento contenente le principali informazioni relative alle operazioni di trattamento svolte dal titolare o dal responsabile del trattamento. Nonostante possa sembrare una incombenza aggiuntiva, avere il registro sotto la propria responsabilità potrebbe rappresentare per il DPO un vantaggio dal punto di vista organizzativo, per il raggiungimento dell'obbiettivo di controllare il rispetto delle norme del Regolamento.

## – 4.3 –

# Designazione

La designazione del *Data Protection Officer*, secondo il Regolamento, può essere effettuata sia dal titolare che dal responsabile del trattamento, oppure congiuntamente. Le Linee Guida consigliano comunque di redigere un documento esplicativo contenete le valutazioni sulle quali si è basata la scelta del DPO, la cui nomina non è sempre ritenuta obbligatoria[39]. È necessario inoltre distinguere tra designazione del DPO da parte di soggetti privati e designazione del DPO da parte di soggetti pubblici.

I soggetti privati sono obbligati a designare un DPO quando le attività principali di cui si occupano il titolare e il responsabile «consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedano il monitoraggio regolare e sistematico degli interessati su larga scala»[40] oppure «consistono nel trattamento, su

[39] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 7; «[…] il Gruppo di lavoro raccomanda a titolari del trattamento e responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina […]»

[40] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 55; Articolo 37 paragrafo 1 lettera b)

larga scala, di categorie particolari di dati»[41]. È importante osservare che, sia il monitoraggio sia il trattamento di categorie particolari di dati ovvero i dati sensibili, rendono la nomina del DPO obbligatoria solo se effettuati su larga scala. Quando si parla di attività principali, si fa riferimento a tutto ciò che è necessario che il titolare ed il responsabile del trattamento mettano in opera per il raggiungimento delle finalità dell'azienda. In questo vengono inclusi anche tutti quei particolari casi in cui le attività compiute ed il trattamento dei dati personali risultano essere inseparabili. Le Linee Guida forniscono degli esempi pratici per spiegare meglio quale sia il legame tra le operazioni eseguite per il raggiungimento degli obiettivi aziendali ed il trattamento dei dati personali.

Ci viene fornito l'esempio di un ospedale, la cui attività principale riguarda la cura del paziente, che però non potrebbe avvenire senza il trattamento dei dati personali dello stesso. Così come il trattamento dei dati personali è assolutamente inseparabile nell'esempio dell'impresa di sicurezza privata, che si occupa della sorveglianza di più centri commerciali e aree pubbliche. In entrambi i casi presentati dalle Linee Guida, il DPO deve essere obbligatoriamente designato[42].

Un altro paramento di cui verificare la presenza per stabilire se la nomina del DPO sia obbligatoria è che il trattamento sia effettuato su "larga scala". Anche in questo caso le Linee Guida forniscono degli esempi per maggiore comprensione, anche in considerazione del fatto che il Regolamento non fornisce una definizione di "larga scala". Ad ogni modo, nelle Linee Guida, vengono elencati dei fattori di cui tener conto, per capire se il trattamento analizzato sia effettuato su larga scala: il numero di soggetti interessati, espresso in percentuale calcolata sulla popolazione di

[41] Parlamento europeo, Consiglio dell'Unione europea; Regolamento 2016/679; Pagina 55; Articolo 37 paragrafo 1 lettera c)

[42] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 9; «[…] gli ospedali sono tenuti a nominare un RPD[DPO] […] [impresa di sicurezza privata] anche l'impresa in oggetto deve nominare un RPD[DPO] […]»

riferimento; il volume e la tipologia dei dati oggetto di trattamento; la durata del trattamento; la portata geografica del trattamento[43].

Nonostante gli esempi forniti dal Gruppo di Lavoro articolo 29 tramite le Linee Guida ci si trova ancora in una fase in cui il concetto di "larga scala" non è perfettamente delineato, e questo lascia spazio ad incertezze, sia sul lato giuridico che sul mercato. Anche per questo motivo, il Gruppo di lavoro intende contribuire alla creazione di uno standard, che contenga delle soglie per la nomina obbligatoria del DPO.

Al momento si deve ritenere soddisfatto il parametro di "larga scala", quando ad esempio, avviene il trattamento di dati relativi agli spostamenti dell'utenza del trasporto pubblico, oppure quando il trattamento dei dati viene effettuato da una banca o da una compagnia assicurativa nello svolgimento delle loro mansioni.

Per quanto riguarda il "monitoraggio regolare e sistematico degli interessati", anche in questo caso non vi è una definizione nel Regolamento, ma tutte le forme di profilazione e tracciamento che avvengono in internet sono da considerarsi di questo tipo. Rientrano in tale categoria anche le operazioni di manutenzione di una rete di telecomunicazioni, il reindirizzamento di email, il tracciamento dell'ubicazione da parte di *app* su dispositivi *mobile* e diverse altre attività, che spaziano dalla pubblicità comportamentale alla domotica, passando dai dispositivi *wearables*[44].

---

[43] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 10

[44] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 11-12; «Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; [...] profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi

Nel caso in cui sia un soggetto pubblico ad effettuare il trattamento di dati personali la designazione è obbligatoria. Infatti, il Regolamento impone la designazione del DPO a tutti gli enti che sono definiti autorità pubbliche, sia di carattere nazionale che di tipo regionale o locale, lasciando spazio alle leggi in materia promulgate da ogni singolo Stato dell'Unione.

Nel caso in cui un'azienda, nonostante la non obbligatorietà, decida di nominare comunque un DPO, quest'ultimo godrà di "pieni poteri" come qualsiasi altro DPO[45].

mobili;[...] monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; [...]»

[45] Gruppo di lavoro articolo 29 per la protezione dei dati; Linee guida sui responsabili della protezione dei dati (WP243); Pagina 7; «Se si procede alla nomina di un RPD[DPO] su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD[DPO] esattamente come nel caso di una nomina obbligatoria»

# Capitolo 5

# Conclusioni

Il Regolamento Generale sulla Protezione dei Dati (GDPR) tra i suoi obiettivi ha quello di fornire una regolamentazione in materia di protezione dei dati personali che sia comune a tutti gli Stati membri dell'Unione europea. Tramite regole più stringenti, che in caso di violazione possono portare anche a pene pecuniarie severe, il GDPR vuole far crescere la fiducia di tutti i cittadini.

Una regolamentazione unica per tutto il territorio comunitario dovrebbe spingere i cittadini a utilizzare, con sempre meno timore, i servizi e i prodotti che necessitano del trattamento di dati personali. Se la fiducia dei cittadini nel prossimo futuro dovesse aumentare, potrebbero nascere delle importanti opportunità per tutto il mercato comunitario.

Ovviamente il raggiungimento di questo obiettivo non è né semplice né tanto meno immediato. Dalla data di pubblicazione in Gazzetta Ufficiale alla data di applicazione del Regolamento sono trascorsi due anni e, in questo periodo, tutte le imprese (ed enti) non in linea con le norme avrebbero dovuto adeguarsi. Non tutte lo hanno fatto e molte affermano che riusciranno ad adeguarsi soltanto entro la fine del 2019.

I diritti dell'interessato sono ciò che il Regolamento, tramite le sue norme, vuole proteggere. Considerando l'avanzamento tecnologico sviluppatosi nel tempo, il legislatore ha deciso di modernizzare gli strumenti normativi finora a disposizione degli Stati membri, portando il titolare del trattamento ad occuparsi della protezione dei dati ancor prima che il trattamento abbia luogo. Essendo il GDPR un Regolamento richiedente particolare attenzione sul fronte della protezione dei dati, il legislatore ha introdotto la figura del *Data Protection Officer*. Il DPO oltre ai propri specifici compiti, ricopre l'importante ruolo di promotore della cultura della protezione dei dati. Deve far capire a tutti coloro che nell'impresa trattano dati personali, che una loro inadempienza può provocare molti più danni di quello che possa sembrare. Deve riuscire a trasmettere loro che non stanno lavorando solo con dei fogli di carta o pezzi di codice dentro un *display*, bensì con informazioni riguardanti le persone, e queste ultime devono essere tutelate.

In questo modo il Regolamento, da un lato impone ad imprese ed enti più vincoli e una maggiore attenzione, ma dall'altro fornisce un valido strumento a tutti i soggetti interessati per veder rispettati i propri diritti.

# Bibliografia

[ 1 ] AA. VV., *Il nuovo Regolamento europeo sulla privacy e sulla protezione dei dati personali,* Zanichelli, Bologna, 2017

[ 2 ] COLOMBO M., *Regolamento privacy UE 2016/679: Principi generali e ruolo del Data Protection Officer,* CreateSpace Independent Publishing Platform, 2017

[ 3 ] FINOCCHIARO G., *La memoria della rete e il diritto all'oblio,* in *Dir. inf.,* Giuffrè, Milano, 2010

[ 4 ] GOVERNO ITALIANO, *Decreto Legislativo n.196 – Codice in materia dei dati personali,* 2003, https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1311248, data ultimo controllo link: Agosto 2018

[ 5 ] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sul diritto alla portabilità dei dati (WP242),* 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48142, data ultimo controllo link: Dicembre 2018

[ 6 ] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida sui responsabili della protezione dei dati (WP243),* 2017, http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48137, data ultimo controllo link: Dicembre 2018

[ 7 ] GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, *Linee guida in materia di trasparenza (WP 260) definite in base alle previsioni del Regolamento (UE) 2016/679,* 2017,

http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025, data ultimo controllo link: Agosto 2018

[ 8 ] PARLAMENTO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Direttiva 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,* 1995, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:31995L0046, data ultimo controllo link: Agosto 2018

[ 9 ] PARLAMENTO EUROPEO, CONSIGLIO DELL'UNIONE EUROPEA, *Regolamento (UE) 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati,* 2016, https://eur-lex.europa.eu/legal-content/it/TXT/?uri=CELEX:32016R0679, data ultimo controllo link: Agosto 2018

[10] STATI MEMBRI, *Carta dei diritti fondamentali dell'Unione europea,* 2016, https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:12016P/TXT, data ultimo controllo link: Agosto 2018