POLITECNICO DI TORINO

Corso di Laurea Magistrale

Ingegneria della Produzione Industriale e dell'Innovazione Tecnologica

Tesi di Laurea Magistrale

Sfide aziendali nell'era del *General Data Protection Regulation*

Candidato: Davide Matera

Relatore: Prof. Stefano Zucca

Anno Accademico: 2018-2019

Indice

Lista delle tabelle

1. Introduzione

1.1. Origine e storia

Il nuovo Regolamento generale sulla protezione dei dati personali, denominato anche GDPR, acronimo di *General Data Protection Regulation*, è stato introdotto mediante la Direttiva n. 679 del 2016, recante "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": esso è entrato in vigore il 24 maggio 2016 ma è divenuto pienamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018. In sostanza, mediante questa nuova normativa il Parlamento Europeo, il Consiglio dell'Unione Europea e la Commissione Europea volevano raggiungere un obiettivo ben preciso ovvero rafforzare e rendere più omogenee le normative riguardanti la protezione dei dati personali all'interno del circuito comunitario.

Il GDPR raffigura la terza normativa che viene emessa in materia di privacy. Di seguito i passaggi che hanno contrassegnato la legislazione sulla privacy.

1996: viene emanata la legge n. 675/1996, la prima legge sulla protezione dei dati personali che stabiliva l'impegno di assunzione delle misure "minime" di sicurezza. Si trattò di una rivoluzione vera e propria dal momento che, per la prima volta, veniva data una definizione, in osservanza dei dettami forniti dalla Direttiva europea 95/46, dei "dati personali" e del loro trattamento secondo norme individuate con l'obbligo di adozione, da parte di coloro che procedevano al trattamento, delle misure di sicurezza.
1999: fa seguito il D.P.R. n. 318 del 28 luglio 1999 il quale definiva le misure di sicurezza. Questa norma provvedeva ad inserire il concetto di trattamento del dato personale, ma aveva il limite di essere sconclusionata e ancora troppo acerba.
2003: viene emanato il D. Lgs. 196/2003 "Codice della privacy". Mediante questo provvedimento la normativa privacy veniva unificata in un solo testo, con un allegato (all. B) all'interno del quale vi erano indicate le misure di sicurezza. il Codice è stato successivamente integrato da molteplici provvedimenti del Garante che ha regolamentato il trattamento in dettagliati settori del mercato. Si è trattato di una norma certamente di rilievo che ha presentato il pregio di plasmare la privacy per i differenti settori di mercato.

2016-2018: il 25 maggio di quest'anno entra in vigore il nuovo Regolamento Privacy, 2016/679 (GDPR).[1]

Il GDPR è indubbiamente una novità che porta con sé innumerevoli implicazioni, innanzitutto una modificazione totale dell'approccio che il soggetto deve avere nei riguardi del trattamento dei dati.

Il GDPR (acronimo per *General Data Protection Regulation*) parte da una prospettiva del tutto differente da quelle assunte precedentemente e pone l'attenzione sulla rilevanza che i dati personali ricoprono nel nostro sistema, qualificati dal Regolamento stesso come diritti fondamentali dell'uomo.

Le conseguenze di queste previsioni sono palesi e implicano un differente approccio che l'individuo deve tenere nel trattamento dei dati.

Tutti i cambiamenti all'organizzazione di un'azienda che si rendessero indispensabili dovranno essere intesi non più come mero costo bensì come vero e proprio investimento.

Il Regolamento è pienamente applicabile all'interno di tutta la Comunità Europea; non dovranno esserci particolari atti dei governi, eccetto per l'adeguamento della normativa interna (sulla scorta dell'art. 13 della L. di delegazione europea 2016 - 2017).

L'arco temporale trascorso tra la data di approvazione (24 maggio 2016) e la sua entrata in vigore (25 maggio 2018) ha palesato come solo scopo quello di permettere l'adeguamento delle imprese pubbliche e private a questa normativa.

Occorre evidenziare che la normativa europea è stata ideata in maniera tale da imporre un continuo controllo e, pertanto, un potenziale adeguamento o cambiamento delle soluzioni adottate e dei sistemi impiegati al fine di assicurare una protezione dei dati personali che sia il più possibile concreta e continua negli anni, nonché allineato con lo sviluppo tecnologico. Ciò sta ad indicare che il processo di adeguamento al GDPR che le aziende e gli enti devono attuare non si è concluso il 25 maggio scorso, bensì diventerà un adempimento costante, in rapporto ad un sistema tecnico e normativo in regolare evoluzione.[2]

Come afferma la stessa Direttiva il GDPR persegue un obiettivo ben preciso ovvero quello di armonizzare le leggi per quanto riguarda la riservatezza dei dati personali in tutta Europa assicurando protezione dei dati di tutti i cittadini dell'Unione Europea e dando a tutte le organizzazioni gli strumenti necessari per assicurare la riservatezza di tali dati. In sostanza, i dati a cui si riferisce questo Regolamento riguardano i dati personali che sono identificati nel nome, nel indirizzo, nell'indirizzo

[1] Amato F., Sbaraglia G., GDPR. Kit di sopravvivenza. Capirlo, applicarlo ed evitare sanzioni sulla privacy e il trattamento dei dati personali, goWare Content Team, 2018.

[2] De Stefani F., Guida pratica al nuovo GDPR, Hoepli, Milano, 2018.

di posta elettronica o, anche, nelle fotografie che riguardano la persona stessa [3]. Anche se tale Regolamento potrebbe apparire, inizialmente, come una novità eredita parte dell'impianto normativo, con qualche piccola modifica della Direttiva 95/46/CE riguardante sempre la protezione dei dati personali. Uno dei cambiamenti più importanti che ha riguardato questo nuova normativa è proprio l'estensione della giurisdizione del Regolamento che viene applicato a tutte quelle organizzazioni che trattano i dati personali di cittadini residenti all'interno del territorio comunitario, indipendentemente da dove sia collocata l'ubicazione di tale organizzazione. Ciò significa che la normativa relativa al GDPR si applica al trattamento dati personali di cittadini comunitari da parte di organizzazioni che non risiedono all'interno del territorio europeo ma che hanno la facoltà di offrire servizi e beni ai residenti dell'Unione Europea [4]. Questa normativa venne presentata per la prima volta dalla Commissione Europea al Parlamento e al Consiglio il 25 gennaio 2012: dopo un periodo di analisi e di aggiustamenti relativi alla normativa nell'aprile 2016 Parlamento e Consiglio approvarono il testo normativo procedendo alla pubblicazione nella Gazzetta Ufficiale dell'Unione Europea che avviene il 4 maggio 2016. Il Regolamento entra in vigore il 24 maggio 2016 e a partire dal 25 maggio scorso è stato applicato, in via diretta, in tutti gli Stati membri. Tra le ragioni che hanno spinto gli organi comunitari a redigere e approvare questo nuovo pacchetto sulla protezione dei dati personali vi è l'ormai famosa inadeguatezza delle disposizioni normative ricomprese all'interno della Direttiva 95/46/CE: ciò è stato affermato ampiamente dalla Commissione Europea all'interno di una sua comunicazione, "*Salvaguardare la privacy in un mondo interconnesso: Un quadro europeo della protezione dei dati per il XXI secolo*". In essa la Commissione stabiliva che il quadro giuridico della Direttiva n. 46 del 1995, pur rivelandosi valido per quanto riguarda gli obiettivi e i principi, ha determinato una frammentazione delle modalità di applicazione della protezione dei dati personali all'interno del circuito comunitario non riuscendo ad eliminare l'incertezza giuridica e la percezione del rischio da parte degli utenti nel momento in cui inseriscono dati personali on line. Inoltre, la precedente Direttiva non creava una normativa armonizzata per tutti gli Stati membri per quanto riguarda le modalità di esercizio del diritto alla protezione dei dati personali e nè attribuiva le competenze idonee alle Autorità nazionali che si occupano della protezione dei dati al fine di assicurare un'applicazione efficace e coerente della normativa. In sostanza, anche se la normativa stabiliva delle precise disposizioni in pratica era molto difficile far valere tali diritti soprattutto per alcuni Stati membri rispetto ad altri e soprattutto attualmente vista la grande diffusione e il grande

[3] TOSHIBA – LEADING INNOVATION, *GDPR: cosa comporta per la vostra azienda*, in *Together information*, 2016.
[4] È fondamentale che tutte le organizzazioni applichino una strategia GDPR – l'inazione non è un'alternativa, in quanto la mancata ottemperanza ai requisiti del GDPR potrà portare a sanzioni fino a 20 milioni di euro o fino al 4% del fatturato mondiale totale annuo.

utilizzo di internet [5]. Unitamente a queste osservazioni, un'altra motivazione che ha spinto gli organi comunitari e redigere tale normativa è identificata negli sviluppi tecnologici e nei nuovi ritmi dettati dalla globalizzazione. In effetti, come ha osservato la Commissione Europea, gli sviluppi tecnologici, che hanno determinato la nascita di internet hanno fortemente inficiato il processo di protezione dei dati personali determinando un aumento della raccolta e della condivisione dei dati. Questa tecnologia ha permesso alle imprese private e alle autorità pubbliche di utilizzare i dati personali nello svolgimento delle loro attività e gli stessi utenti privati, mediante internet, hanno la possibilità di rendere pubbliche numerose informazioni personali che gli riguardano direttamente. In questo modo, tale tecnologia associata ad internet ha modificato fortemente le relazioni sociali mutando gli ambienti on-line. Formulando tale comunicazione e presentando un progetto relativo al nuovo pacchetto giuridico, la Commissione era fortemente convinta che i tempi fossero ormai maturi per realizzare un quadro giuridico più solido e coerente per quanto riguarda la protezione dei dati personali all'interno dell'Unione predisponendo tutti quegli strumenti necessari e quelle misure di attuazione che consentissero, al contempo, lo sviluppo dell'economia digitale nel mercato interno, il controllo da parte delle persone fisiche dei propri dati personali, il rafforzamento della certezza giuridica e la riduzione, quanto possibile, degli oneri amministrativi a vantaggio delle imprese [6]. La Commissione, infatti, unitamente al Parlamento Europeo e al Consiglio Europeo era fortemente convinta (a ragion del vero) che la disciplina attuata fino a quel momento non fosse in grado di fronteggiare e far fronte ad alcune importanti esigenze che adesso riguardano cittadini, imprese e istituzioni pubbliche e a numerose problematiche che adesso potranno essere risolte. Inoltre, occorre fare un ulteriore osservazione questa nuova normativa in grado di disciplinare, in termini nuovi, il trattamento dei dati personali ha sostituito, come abbiamo potuto vedere, la Direttiva 95/46/CE che è stata sostituita non con un'altra direttiva ma con un Regolamento: infatti, questo nuovo pacchetto è stato ricompreso all'interno del Regolamento n. 679 del 2016. L'idea di sostituire la Direttiva con un Regolamento è un fattore di notevole rilievo poiché come ha affermato la stessa Commissione il Regolamento si qualifica come strumento più idoneo per disciplinare, dal punto di vista giuridico, la protezione dei dati personali all'interno dell'Unione Europea soprattutto perché è stata decisa un'applicazione diretta di quanto in esso disposto, operazione che attribuirà maggiore certezza giuridica grazie all'introduzione di norme armonizzate, al miglioramento della tutela dei diritti fondamentali delle

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

[6] Queste sono infatti le premesse essenziali affinché il mercato interno funzioni correttamente e possa conseguentemente stimolare la crescita economica, creare occupazione e promuovere l'innovazione.

persone fisiche e alla garanzia di un corretto funzionamento del mercato interno [7]. La precedente direttiva non aveva determinato un'armonizzazione di tutta la normativa dell'Unione, né le conseguenti modalità di esercizio del diritto alla protezione dei dati personali e né le competenze conferite alle Autorità nazionali nonostante, ad oggi, far valere tali diritti nel mondo di internet, si qualifichi come una missione più difficile in alcuni Paesi rispetto ad altri e ciò dipende soprattutto della natura dello strumento giuridico in questione che non è immediatamente applicabile, a differenza del nuovo Regolamento. In effetti, la Direttiva necessitò delle leggi di recepimento da parte degli Stati membri che, in virtù dell'articolo 288 del TFUE, sono vincolati per quanto riguarda il risultato da raggiungere ma non per quanto riguarda la forma e i mezzi. Questa precisazione può far emergere delle differenze significative tra i vari Paesi membri per quanto riguarda il processo di trasposizione della Direttiva. Con il Regolamento in questione le cose sono fortemente cambiate: esso viene presentato come obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri, senza la richiesta di leggi di recepimento cosa che, come era nelle intenzioni delle istituzioni europee, ha permesso di attribuire maggiore certezza normativa e ridurre la frammentazione. In sostanza, se il Regolamento riuscirà a raggiungere risultati più significativi rispetto a quelli che sono stati conseguiti dalla precedente Direttiva del 1995 questo successo sarà determinato non solo dal contenuto in sede il Regolamento ma anche dalla natura dello strumento giuridico stesso [8].

1.2. Obiettivi del GDPR

Gli obiettivi perseguiti dal Regolamento sono specificati all'interno dell'articolo 1 che afferma quanto segue: "*1. Il presente regolamento stabilisce norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché norme relative alla libera circolazione di tali dati. 2. Il presente regolamento protegge i diritti e le libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali. 3. La libera circolazione dei dati personali nell'Unione non può essere limitata né vietata per motivi attinenti alla protezione delle persone fisiche con riguardo al trattamento dei dati personali*". In sostanza il Regolamento detta delle disposizioni specifiche al fine di assicurare protezione per quanto riguarda il trattamento dei dati personali e la libera circolazione di suddetti dati, assicurando la salvaguardia dei diritti e delle libertà

[7] BASSOLI E., *La nuova privacy GDPR dopo il D. lgs. 10 agosto 2018, n.101. Guida teorico-pratica con schemi riassuntivi e formulario dei principali adempimenti*, Dike Giuridica, Milano, 2018.
[8] RUGANI G., *Il Nuovo Pacchetto europeo sulla protezione dei dati personali: dalle origini al diritto all'oblio*, Università degli studi di Pisa, Pisa, 2017.

fondamentali delle persone fisiche in questo ambito. Al terzo comma tale disposizione stabilisce che la libera circolazione dei dati personali non può essere limitata o vietata per far valere la protezione delle persone fisiche per quanto riguarda il trattamento dei dati personali [9]. Da questa disposizione normativa emerge il duplice obiettivo ovvero la protezione delle persone fisiche per quanto riguarda il trattamento dati personali e la libera circolazione dei dati: questi obiettivi vengono fortemente correlati ad altri importanti elementi identificati nel Regolamento ovvero:

- la garanzia di correttezza e trasparenza secondo la quale i dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato cosa che richiede al responsabile del trattamento di spiegare all'utente interessato il procedimento che riguarderà il trattamento dei suoi dati. Tale spiegazione deve essere trasparente e di facile comprensione e lo stesso processo di trattamento deve avvenire conformemente a quanto descritto all'interessato;
- la limitazione delle finalità: la normativa stabilisce che i responsabili e i titolari del trattamento hanno la facoltà di raccogliere i dati personali solo per seguire finalità determinate, esplicite e legittime: in questo modo i dati devono essere trattati seguendo un procedimento che sia completamente compatibile con suddette finalità. Da ciò si evince che il trattamento dei dati è esclusivamente limitato alle finalità per cui tali dati sono stati raccolti inizialmente, facendo emergere il divieto di implementare un trattamento per una finalità diversa o in una fase successiva, senza che sia stata concessa l'autorizzazione da parte dell'utente interessato;
- la minimizzazione dei dati: la normativa stabilisce che sono soggetti a trattamento solo i dati adeguati e pertinenti: Infatti, la loro raccolta si limita solamente a quanto necessario per il perseguimento delle finalità per cui i dati vengono trattati. I responsabili al trattamento non possono raccogliere una quantità importante di dati per assicurarsi un uso futuro o per creare un profilo dell'utente a meno che ciò non sia necessario per raggiungere finalità legali. La minimizzazione dei dati risponde all'obiettivo di limitazione delle finalità cosa che impone alle aziende di raccogliere solo i dati strettamente necessari per raggiungere le finalità senza spingersi al di là del necessario [10];
- la garanzia di esattezza: è di fondamentale importanza che la normativa si basi sul principio di esattezza e che assicuri alti standard di qualità nel trattamento dei dati: in sostanza, si

[9] DE STEFANI F., *Le regole della privacy. Guida pratica al nuovo GDPR*, Hoepli, Milano, 2018.
[10] TOSHIBA – LEADING INNOVATION, *GDPR: cosa comporta per la vostra azienda*, op. cit.

impone, non solo trattare adeguatamente i dati, ma anche di rivederli e aggiornarli periodicamente;

- la limitazione della conservazione: la normativa stabilisce che i dati personali devono essere conservati in un formato che permetta l'identificazione dei soggetti interessati per un arco di tempo che non sia superiore al conseguimento delle finalità per i quali sono stati raccolti. Da ciò si evince che le aziende siano chiamate a controllare e verificare periodicamente i dati in loro possesso, cancellando i dati che non sono più necessari per le finalità per le quali erano state precedentemente raccolti;
- la garanzia di integrità e riservatezza: la violazione di questa parte della disposizione. Determina l'applicazione, nei confronti dei colpevoli, di pesanti sanzioni pecuniarie. In effetti, la normativa ribadisce tra i suoi obiettivi la necessità di trattare i dati in modo da assicurare loro sicurezza e protezione, mediante misure tecniche e organizzative adeguate, salvaguardandoli da trattamenti non autorizzati, da trattamenti illeciti o dalla perdita di tali danni. Questa è una delle parti più importanti della disposizione nei confronti della quale il responsabile trattamento deve prestare forte attenzione soprattutto al giorno d'oggi dove il mondo di internet con le sue insidie mette a repentaglio la sicurezza dei dati. Di conseguenza, i responsabili sono chiamati a predisporre un'adeguata politica di sicurezza dei dati che dia loro gli strumenti adeguati a segnalare eventuali disposizioni delle disposizioni contenute all'interno del regolamento [11].

1.3. Il concetto di "dato personale"

Il regolamento, come abbiamo potuto comprendere dalla lettura del primo paragrafo, regola il trattamento dei dati personali.

Ma cosa vogliamo dire, precisamente, quando parliamo di dato personale?

La definizione di dato personale ci viene fornita dall'art. 4 del Regolamento e si tratta di una norma diretta a fornire una puntuale indicazione circa le definizioni dei termini impiegati dal Regolamento medesimo.

A norma di questo articolo, pertanto, per dato personale di 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 riferimento a un identificativo come il nome, un*

[11] *Ibidem*.

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".[12]

In particolar modo, si tratta di dati che fanno riferimento a persone fisiche in vita (infatti, il trattamento dei dati inerente ad individui deceduti è estromesso dall'ambito del Regolamento) identificate o identificabili.

Raffigurano dati personali anche tutte quelle informazioni che, correlate tra loro, rendono possibile l'identificazione della persona cui fanno riferimento.

Tabella 1 – esempi di dati personali e non personali

Esempi di dati personali	• Nome e cognome • Indirizzo di casa • Indirizzo e-mail (personale anche se con dominio aziendale) • Numero della carta di identità • Indirizzo IP • Il numero di un badge aziendale
Esempi di dati non personali	• Indirizzo e-mail generico dell'azienda • Numero di iscrizione alla CCIA • Dati anonimizzati in modo irreversibile

Anonimizzare un dato vuol dire far sì che quel dato non sia più riferibile ad una singola persona. Ne consegue, dunque, che il dato è veramente anonimo solamente nel caso in cui il processo di anonimizzazione sia irreversibile, ossia non sia possibile risalire con alcun mezzo e tecnologia, al riconoscimento della persona.[13]

1.4. Struttura

Il GDPR è composto da 99 articoli, suddivisi in 11 capitoli, preceduti da 173 "considerando". Di seguito come sono strutturati:

Capo I: Disposizioni generali (artt. 1 - 4);

[12] Art. 4, Reg. 698/2016
[13] De Stefani F., Guida pratica al nuovo GDPR, op. cit.

Capo II: Principi (artt. 5 - 11);

Capo III: Diritti dell'interessato (artt. 12 - 23);

Capo IV: Titolare del trattamento e responsabile del trattamento (artt. 24 - 43);

Capo V: Titolare del trattamento di dati personali verso paesi terzo o organizzazioni internazionali (artt. 44 - 50);

Capo VI: Autorità di controllo indipendenti (artt. 51 - 59);

Capo VII: Cooperazione e coerenza (artt. 60 - 76);

Capo VIII: Mezzi di ricorso, responsabilità e sanzioni (artt. 77 - 84);

Capo IX: Disposizioni relative a specifiche situazioni di trattamento (artt. 85 - 91);

Capo X: Atti delegati e atti di esecuzione (artt. 92 - 93);

Capo XI: Disposizioni finali (artt. 94 - 99).[14]

1.5. The right to be alone: evoluzione del "diritto alla privacy"

Solitamente si ha la tendenza di dire a chi si intromette nelle nostre situazioni private "sta violando la mia privacy". Invero stiamo commettendo un errore nel ritenere che la salvaguardia della nostra privacy venga circoscritta solamente a questo.
Come sosteneva nel 1998 il primo Garante per la protezione dei dati personali italiano, il Professore Stefano Rodotà nel suo discorso tenuto presso il liceo Isacco Newton nella Capitale: «*quello della privacy non è più soltanto il diritto a essere lasciati soli, ma è il diritto di decidere liberamente della propria vita privata. Una questione, quindi, di capitale importanza*»[15].
Tutto ha inizio con un saggio, scritto da due giovani di Boston Samuel Warren e Louis Brandeis, che ha fatto la sua prima apparizione il 15 dicembre 1890 sulla "Harvard Law Review", *The Right to privacy*.
Furono loro a ideare "*the Right to be let alone*", moderna enunciazione dello *ius solitudinis*, e cioè il diritto ad essere lasciati da soli, in modo tale da godere in pace della propria vita.
Attualmente, il diritto alla privacy, in virtù anche del contributo di preparati e qualificati esperti del diritto è andato sempre più sviluppandosi, andando ad ampliarsi fino ad includere il diritto di

[14] Amato F., Sbaraglia G., GDPR. Kit di sopravvivenza. Capirlo, applicarlo ed evitare sanzioni sulla privacy e il trattamento dei dati personali, op. cit.
[15] Ibidem.

monitorare la circolazione dei propri dati personali. Detto in altre parole: ai nostri giorni è il diritto, basilare nell'era di internet, che consente ad ogni persona di esercitare un controllo sulle informazioni che concernono la propria persona.

Lo stesso Garante italiano per la protezione dei dati personali definisce la protezione dei dati come un "diritto di libertà"; un diritto di cui ognuno di noi, prima di reclamarne tutela, deve averne cognizione per mezzo di un impegno diretto a comprendere i suoi contorni ed il suo significato.[16]

[16] Ibidem.

2. Il contenuto

2.1. Dal diritto alla "privacy" al diritto alla "protezione dei dati personali"

Nella normativa precedente la protezione dei dati personali era strettamente collegata alla tutela dei diritti e delle libertà fondamentali e un collegamento speciale era stato istituito fra tale e protezione e la tutela del diritto alla privacy. Questa impostazione giuridica ha subito una modifica con la pubblicazione del Regolamento n. 679 del 2016 che ha conservato l'esistenza della protezione dei dati personali e la sua correlazione con la tutela dei diritti e delle libertà fondamentali ma ha eliminato la correlazione esistente alla privacy: al suo posto il Regolamento ricomprende il diritto alla protezione dei dati personali. Come ha evidenziato la normativa precedente il diritto alla protezione dei dati personali comprende 6 elementi essenziali; il requisito del principio di lealtà nel trattamento dei dati, il requisito del trattamento solo per le finalità determinate, il requisito del fondamento legittimo previsto dalla legge, il consenso del soggetto interessato, il diritto di accesso ai dati, il diritto di ottenere la loro rettifica e il controllo da parte di un soggetto indipendente [17].

Sulla base di questi elementi emerge che il diritto alla protezione dei dati personali mantiene legami molto stretti con il diritto di accesso ai dati. Questo diritto ricomprende non solo la possibilità del soggetto di accedere ai dati e di esercitare in ferreo controllo, ovvero la possibilità di ottenerne la rettifica se inesatte, ma include anche una serie di obblighi in capo al titolare del trattamento. L'idea di fondo che viene promossa mediante questa normativa è quella di non proteggere i dati esclusivamente da ingerenze esterne, ma anche di consentire al soggetto interessato esercitare un ferreo controllo su di essi [18].

Sulla base di questo presupposto alcuni esperti giuridici hanno criticato l'uso che viene fatto dell'espressione "diritto alla protezione dei dati personali", affermando che sarebbe più opportuno parlare, giuridicamente, di "diritto al controllo dei dati personali". In ogni caso, anche se il controllo non viene mantenuto nella formula giuridica, esso è previsto dall' impianto normative [19].

Come è stato affermato il diritto alla protezione dei dati personali, previsto dal Regolamento, oltre a escludere l'ingerenza altrui e assicurare una tutela negativa, concretizza in capo al soggetto interessato dei poteri di controllo e di intervento. Da ciò emerge una tutela dinamica che segue i movimenti e la

[17] RICCIO G. M., SCORZA G. e BELISARIO E., *GDPR e normativa privacy. Commentario*, Ipsoa, Milano, 2018.
[18] RUGANI G., *Il Nuovo Pacchetto europeo sulla protezione dei dati personali: dalle origini al diritto all'oblio*, op. cit.
[19] *Ibidem*.

circolazione stessa dei dati. La definizione di questo approccio ha delle ricadute significative anche nei confronti di altri importanti istituti che vengono disciplinati dal regolamento come ad esempio il diritto alla portabilità dei dati, che ritroviamo all'interno dell'articolo 20, che afferma che al fine di rafforzare il controllo sui propri dati è necessario che il soggetto interessato abbia il diritto di ricevere in un formato strutturato e leggibile da dispositivo automatico i dati personali che lo riguardano che ha fornito a un titolare del trattamento se, tali dati sono stati trattati con mezzi automatizzati.

Al medesimo ambito appartengono gli obblighi di notifica all'autorità di controllo, contenuti all'interno dell'articolo 33, e gli obblighi di comunicazione al diretto interessato, contenuti all'interno dell'articolo 34. La normativa vuole evitare, in qualunque modo, che si verifichi una violazione dei dati personali, evenienza che se non viene affrontata in maniera adeguata e tempestiva può provocare danni fisici, materiali e immateriali alle persone fisiche a cui appartengono i dati nonché anche una perdita del controllo dei dati che li riguardano in prima persona [20].

Pertanto, come è possibile osservare la tutela che viene predisposta non è statica, ma dinamica e non viene assicurata esclusivamente ai dati che sono relativi alla vita privata del soggetto, ma viene assicurata ai dati personali in generale. La normativa del regolamento, quindi, a differenza della normativa precedente ha predisposto una tutela non parziale, ma completa dei dati personali. Il diritto alla vita privata o alla privacy non viene totalmente eliminato ma viene sempre considerato come strettamente connesso alla protezione dei dati personali, pur essendo entrambi dei diritti autonomi [21].

2.2. I principi

Il Capo II del Regolamento 2016/679, che va dall'Articolo 5 all'Articolo 11, concerne i "Principi". La norma di apertura di tale Capo è conforme all'Articolo 6 della Direttiva 95/46/CE, il quale a sua volta rinvia all'Articolo 5 della Convenzione 108; tutte e tre le disposizioni, infine, presentano rilevanti somiglianze con gli articoli 7, 8 e 9 delle Linee guida OCSE, e anche con le risoluzioni 1973-1974 del Consiglio d'Europa.

L'Articolo 5 del Regolamento racchiude infatti una lista di tutti i principi reggenti la materia, e per la sua rilevanza merita di essere riportato:

Art. 5 – Principi applicabili al trattamento dei dati personali

[20] MARINI P., *GDPR: il nuovo regolamento europeo sulla privacy*, Wolters Kluwer Italia, Milano, 2018.
[21] *Ibidem*.

«1. I dati personali sono:

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

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

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

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

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

2. Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»)».[22]

Le difformità più rilevanti che possono riscontrarsi tra l'articolo appena trscritto e l'Articolo 6 della Direttiva 95/46/CE sono due: l'inserimento della lettera f), riservata ai principi di "integrità" e "riservatezza", ma in particolar modo l'introduzione, alla lettera a), del principio di "trasparenza".

[22] Art. 5 GDPR - Principi applicabili al trattamento di dati personali, Altalex, 12 aprile 2018, in http://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali

Nel suo lavoro di trasformazione, il legislatore europeo si palesa molto scrupoloso a quest'ultimo principio: non solo lo inserisce all'Articolo 5, ma rivolge ad esso un'opportuna Sezione. Questa Sezione, la numero 1 del Capo III ("Trasparenza e modalità"), si forma di un solo articolo (il 12), il quale aumenta e intensifica gli obblighi di trasparenza in capo al titolare del trattamento.

2.3. Il principio di liceità e le condizioni per il consenso

Il principio di liceità del trattamento dei dati personali dispone la loro trattazione nell'osservanza delle leggi, anche quelle che disciplinano determinati settori (è il caso dello Statuto dei lavoratori). Tale principio poggia principalmente sull'articolo 52 della Carta dei diritti dell'UE:

> "*Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare il contenuto essenziale di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui*".

L'art. 5 del regolamento generale europeo, infatti, come anticipato sopra dispone che i dati personali debbano essere trattati "*in modo lecito, corretto e trasparente nei confronti dell'interessato*". Pertanto, il trattamento deve:

- essere fedele alla legge;
- raggiungere un fine legittimo;
- rivelarsi indispensabile all'interno di una società democratica al fine di raggiungere un fine legittimo.

Relativamente al requisito conclusivo la giurisprudenza della CEDU stabilisce inoltre che determinati freni (quali la misura di sorveglianza) debbano considerarsi rigorosamente essenziali al fine di ricavare informazioni altrettanto essenziali in quella determinata operazione (sent. Szabo e Vissy c. Ungheria).

L'articolo 5 della Convenzione 108 e l'articolo 6 del Regolamento, catalogano le condizioni di liceità del trattamento in quanto circoscrizione all'esercizio del diritto alla protezione dei dati personali. L'articolo 6 elenca le basi giuridiche del trattamento. Nel dettaglio, il capoverso 2 cataloga le ipotesi

nelle quali gli Stati membri possono disporre condizioni aggiuntive rispetto alla normativa europea, inserendo in tal modo una condizione di elasticità a beneficio delle norme nazionali.[23]

Una importante novità, invece, è raffigurata dall'Articolo 7 del Regolamento, "*Condizioni per il consenso*", il quale puntualizza, per ciò che concerne la liceità del trattamento, le condizioni alle quali l'interessato può palesare e revocare il proprio consenso.

In particolare, se l'autorizzazione dell'interessato viene data nell'ambito di una comunicazione scritta che va a toccare anche altri temi, la domanda di consenso deve essere avanzata in modo tale che sia riconoscibile rispetto alle altre materie, chiaro e agevolmente raggiungibile, impiegando un linguaggio accessibile e trasparente[24].

Con lo stesso agio con cui è stato dato il consenso, deve essere poi possibile revocarlo; in ogni occasione può essere esercitato il diritto di revoca, ma la revoca del consenso non va a pregiudicare la liceità del trattamento fondata sul consenso precedente rispetto alla revoca medesima[25] (cosa di cui l'interessato è avvisato in un momento anteriore rispetto a quello del consenso).

Rilevante anche il paragrafo 1 dove viene posto in capo al titolare del trattamento, l'onere della prova circa il fatto che l'interessato ha dato il proprio consenso al trattamento dei propri dati personali.

In definitiva nel Regolamento spicca ancora di più l'importanza del consenso, elemento basilare già nella Direttiva 95/46/CE. Questa centralità, occorre sottolinearlo, non è propria della Convenzione 108, bensì origina dall'esperienza tedesca.

2.4. I dati sensibili

Tra i dati personali protetti nel nuovo Regolamento UE 2016/679 ne troviamo certuni che necessitano di una più intensa salvaguardia, in virtù della loro attitudine nel manifestare aspetti correlati alla sfera più intima della persona. Si tratta di quei dati che all'interno del nostro Codice Privacy sono stati definiti con il termine di dati sensibili e che attualmente invece, nel GDPR, diventano dati particolari.

La rubrica dell'articolo 9 dispone infatti

> "*trattamento di categorie particolari di dati personali*": sono questi dati che riferiscono "*l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o*

[23] Liceità del trattamento, Protezione dati personali. Data protection, 26 luglio 2017, in https://protezionedatipersonali.it/liceita-del-trattamento
[24] Regolamento 2016/679, Articolo 7 paragrafo 2.
[25] Ibid. paragrafo 3.

> *l'appartenenza sindacale, nonché […] dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*"[26].

Le categorie coincidono con quelle esposte nella esplicitazione degli (ex) dati sensibili, ma con l'inserimento dei dati genetici e biometrici.

Queste due tipologie di dati vengono richiamati anche all'interno del D. Lgs. 196/2003 e vengono fatti rientrare in quel varietà di dati che, sebbene non vengono fatti rientrare in quelli sensibili, sono stati oggetto (fino al momento dell'entrata in vigore del GDPR) di una peculiare salvaguardia in quanto soggetti alla notifica preventiva al Garante ai sensi dell'art. 37.

Il dato biometrico, in particolar modo, ha subito svariati provvedimenti sia per mano del nostro Garante che del Gruppo di lavoro ex articolo 29. Si notano, infatti, in numero sempre maggiore, strumenti per la raccolta di dati biometrici

> «*quali impronte digitali, forma dell'iride, emissione vocale o firma grafometrica, a scopo di accertamento dell'identità personale, di accesso a servizi digitali e sistemi informativi o per finalità di controllo dell'accesso a locali*»[27]

Sono diverse le basi giuridiche che convalidano il trattamento dei dati particolari (che troviamo enumerate al paragrafo 2 dell'articolo 9 del GDPR), nonché in maggior misura specifiche, rispetto a quelle che ratificano il trattamento dei dati cc.dd. comuni di cui all'articolo 6.

Vi risultano, tanto per menzionarne alcune: la protezione di un interesse indispensabile dell'interessato; «*l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria; l'interesse pubblico rilevante sulla base del diritto dell'UE o degli Stati membri; l'esigenza del trattamento in materia di diritto del lavoro, di protezione e sicurezza sociale o per scopi inerenti la medicina preventiva o quella del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi , assistenza o terapia sanitaria o sociale*»[28].

Se la finalità perseguita dal titolare non può essere fatta rientrare in alcuna delle categorie elencate dall'art. 9, par. 2 lett. b) – j) del Regolamento il trattamento può essere praticato sulla scorta del

[26] Art. 9, GDPR.
[27] Si veda, in particolare, il Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014 del garante per la protezione dei dati personali ed il relativo allegato A "Linee guida in materia di riconoscimento biometrico e firma grafometrica", in I dati sensibili tra Codice Privacy e GDPR, articolo di Zabeo E., 28 maggio 2018, in https://www.cyberlaws.it/2018/dati-sensibili-gdpr-nuovo-codice-privacy/
[28] Ibidem.

consenso espresso e chiaro dell'interessato, che ha bisogno di un elemento aggiuntivo rispetto al mero consenso.

La locuzione espresso, così come chiarito dal WP 29, fa riferimento alle modalità di espressione, per cui l'interessato deve comunicare una chiara asserzione di consenso, ad esempio mediante una comunicazione firmata o, nell'ipotesi di servizi online, mediante riempimento di un *form* o *scanning* di una documentazione riportante il proprio nome e cognome o attraverso l'utilizzo della firma elettronica.

Ulteriore modalità può constare nel controllo del consenso mediante un duplice passaggio: ad esempio il titolare del trattamento che desidera trattare dati particolari chiede che l'interessato invii una e-mail con una dichiarazione di consenso e, in un secondo momento, trasmette all'interessato un collegamento ipertestuale o un messaggio con un codice di controllo per permettergli di convalidare ancora una volta la propria volontà.[29]

Nell'ultima bozza di decreto presentata il 10 maggio, viene puntualizzato il fatto che la parola dati sensibili deve ora riferirsi ai dati che vengono menzionati nell'articolo 9 del Regolamento.

Il nostro Legislatore ha poi disposto, a compimento di quanto sancito dall'articolo 9 comma 4 del Regolamento (che permette agli stati membri di inserire ulteriori condizioni concernenti il trattamento di dati biometrici, genetici o concernenti la salute) l'impegno di assumere delle misure di garanzia per il trattamento di questi dati, le quali devono essere approntate, ogni biennio, con puntuale provvedimento del Garante, il quale dovrà prendere nella giusta considerazione le migliori pratiche inerenti alla protezione dei dati e del progresso scientifico e tecnologico nel settore oggetto delle misure.

Viene meno, inoltre, qualsivoglia riferimento al consenso per il trattamento di dati sanitari che sia eseguito per finalità di protezione della salute e integrità fisica dell'interessato o di terzi o della comunità: questo trattamento viene ritenuto legittimo, e quindi consentito, quando realizzato ai sensi dell'art. 9 par. 2 lett. h) e i)[30], senza quindi alcun bisogno di acquisire il consenso.

[29] Article 29 Working Party Guidelines on consent under Regulation 2016/679 Adopted on 28 November 2017 and last Revised and Adopted on 10 April 2018, in I dati sensibili tra Codice Privacy e GDPR, articolo di Zabeo E., 28 maggio 2018, in https://www.cyberlaws.it/2018/dati-sensibili-gdpr-nuovo-codice-privacy/

[30] «*ossia per scopi di medicina preventiva o medicina del lavoro, valutazione dell'abilità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o socialio per motivi di interesse pubblico nella sanità pubblica*», in I dati sensibili tra Codice Privacy e GDPR, articolo di Zabeo E., 28 maggio 2018, in https://www.cyberlaws.it/2018/dati-sensibili-gdpr-nuovo-codice-privacy/

Questo aspetto si pone si allinea indubbiamente con quella che è l'anima del nuovo Regolamento Europeo, dalla cui lettura affiora come il consenso sia solamente uno dei caposaldi giuridici che ratificano il trattamento dei dati personali, da non impiegare «*quando il trattamento basi la sua legittimità all'interno del contratto, in un obbligo di legge o, nel caso dei dati particolari, in una delle finalità menzionate dall'articolo 9 par. 2, lett. b) – j) del GDPR*».[31]

2.5. I diritti dell'interessato

Le modalità

I modi per poter esercitare i diritti spettanti agli interessati vengono fissati all'interno degli artt. 11 e 12 del Regolamento.

- Termine per la risposta. Per tutti i diritti, incluso quello di accesso, il termine per la risposta è di un mese, e può essere esteso fino a tre mesi nei casi particolarmente difficili. Il titolare ha l'obbligo di fornire un riscontro all'interessato entro un mese dalla richiesta, anche se si tratta di rifiuto.
- Riscontro. Il riscontro all'interessato deve normalmente realizzarsi per iscritto anche per mezzo di strumenti elettronici che ne rendono più agevole l'accessibilità, e può essere fornito a voce solamente se ciò è voluto dall'interessato stesso.
- La risposta che viene data dall'interessato deve essere sintetica, e quindi essenziale, chiara e facilmente comprensiva, deve impiegare espressioni facili da capire per tutti.
- Misure per facilitare l'esercizio dei diritti. Il titolare del trattamento deve semplificare l'esercizio dei diritti da parte dell'interessato, impiegando qualsiasi misura a ciò adeguata. Benché sia unicamente il titolare a dover dare riscontro nel caso di esercizio dei diritti, il responsabile deve assolutamente cooperare con il titolare relativamente all'esercizio dei diritti degli interessati.
- Gratuità per l'esercizio dei diritti. Quest'ultimo è, generalmente, gratuito per l'interessato, sebbene possano manifestarsi alcune eccezioni.
- Informazioni. Al titolare viene riconosciuto il diritto a richiedere tutte le informazioni essenziali all'individuazione dell'interessato, e quest'ultimo ha il dovere di somministrarle, secondo adeguate modalità.

[31] I dati sensibili tra Codice Privacy e GDPR, articolo di Zabeo E., 28 maggio 2018, in https://www.cyberlaws.it/2018/dati-sensibili-gdpr-nuovo-codice-privacy/

- Deroghe. Risultano consentite deroghe ai diritti ammessi dal Regolamento, ma solamente sul fondamento di disposizioni normative nazionali, ai sensi dell'articolo 23 e di altri articoli inerente a determinati e ambiti.

Diritto di accesso (art. 15)

- Il diritto di accesso stabilisce sempre e comunque il diritto ad avere una copia dei dati personali oggetto di trattamento.
- Tra le diverse informazioni che il titolare deve dare non si individuano le "modalità" del trattamento, mentre deve essere indicata la durata di conservazione prefissata o i criteri impiegati per definire questo periodo, e inoltre le garanzie utilizzare nel caso di trasferimento dei dati verso Paesi terzi.

Diritto di cancellazione o diritto all'oblio (art.17)

- Il diritto "all'oblio" si palesa come un diritto volto alla rimozione dei propri dati personali in modo rafforzata. Viene previsto, infatti, l'obbligo per i titolari (nel caso in cui abbiano pubblicato i dati personali dell'interessato: ad esempio, rendendoli pubblici all'interno di un sito web) di informare della richiesta di rimozione altri titolari che trattano i dati personali rimossi, inclusi "*qualsiasi link, copia o riproduzione*".
- Risulta più vasto rispetto a quello già riconosciuto all'art. 7, comma III, lettera b), del Codice della privacy, dal momento che l'interessato ha il diritto di chiedere la rimozione dei propri dati, ad esempio, anche in un momento successivo a quello della revoca del consenso al trattamento.

Diritto di limitazione del trattamento (art. 18)

- Raffigura un diritto differente e più ampliato rispetto al "blocco" del trattamento già stabilito dall'art. 7, comma III, lettera a), del Codice della Privacy. In particolare, può essere esercitato non soltanto nel caso di trasgressione dei presupposti di liceità del trattamento (quale possibilità alla rimozione dei dati stessi), ma anche nell'ipotesi in cui l'interessato fa richiesta di rettifica dei dati o si oppone al loro trattamento ai sensi dell'art. 21 del Regolamento.
- Scartata la conservazione, ogni ulteriore trattamento del dato di cui viene domandata la limitazione è assolutamente proibito, eccetto il caso in cui si manifestino particolari circostanze (quali il consenso dell'interessato, l'accertamento diritti nell'ambito giudiziario, la salvaguardia dei diritti di altra persona fisica o giuridica, l'interesse pubblico rilevante).

Diritto alla portabilità dei dati (art. 20)

- Raffigura un diritto "nuovo" riconosciuto dal Regolamento, sebbene non sia completamente ignoto ai consumatori (basta pensare alla portabilità del numero di telefono).
- Non viene applicato ai trattamenti non automatizzati e vengono stabilite peculiari condizioni per il suo esercizio. In particolare, risultano portabili solamente i dati trattati mediante il consenso dell'interessato ovvero sulla scorta di un contratto redatto con l'interessato e solamente i dati che siano stati "forniti" dall'interessato al titolare.
- Il titolare deve avere la possibilità di trasferire direttamente, a un altro titolare stabilito dall'interessato, i dati portabili, sempre se ciò si riveli tecnicamente fattibile.

Consenso al trattamento dei dati da parte dei minori di 14 anni

Il consenso al trattamento potrà essere esplicitato dai minori al momento del compimento del 14esimo anno di età, in rapporto all'offerta diretta di servizi della società dell'informazione. Al di sotto del 14esimo anno si età, il trattamento risulta consentito a patto che sia prestato da chi esercita la responsabilità genitoriale (genitore legalmente esercente o tutore).

Eredità del dato in caso di decesso

Il decreto che adegua la nostra normativa a quella europea, inserisce il diritto all'eredità del dato nel caso in cui si verifichi il decesso, il quale potrà essere esercitato "*da chi ha un interesse proprio, o agisce a tutela dell'interessato, in qualità di suo mandatario, o per ragioni familiari meritevoli di protezione*".[32]

[32] GDPR: i diritti degli interessati, diritti e risposte per comprendere e risolvere, WoltersKluwer, in http://www.dirittierisposte.it/Schede/Tutela-della-privacy/Diritti/gdpr_i_diritti_degli_interessati_id1173414_art.aspx#Diritto%20di%20cancellazione%20o%20diritto%20all%C2%BFoblio%20(art.17)

3. Impatto del GDPR sulle aziende

3.1. Implementazione

In ambito aziendale, è stato rilevato che il nuovo Regolamento Europeo sulla protezione dei dati personali, a differenza Decreto Legislativo n. 196 del 2003, non prevede l'implementazione di misure minime di sicurezza poiché il legislatore ha preferito includere, all'interno di questa normativa, alcune azioni stringenti al titolare del trattamento dei dati, nei cui confronti sono aumentate tutte le responsabilità relative all'accountability. Proprio l'attribuzione di una maggiore responsabilità ha previsto una preventiva analisi dei rischi nonchè l'adozione di tutte le misure organizzative e tecnologiche che permettono di implementare il GDPR.

In sostanza, le aziende sono chiamate ad implementare un sistema che ricomprende l'analisi del rischio dei dati trattati mediante l'adozione, in ambito aziendale, di un concetto assoluto e dinamico riguardante la protezione delle persone fisiche nel momento in cui viene implementato il trattamento dei loro dati personali. Tale approccio richiede l'implementazione di competenze che attraversano vari ambiti: giuridico, informatico e organizzativo. I cambiamenti più rilevanti che sono introdotti riguardano, oltre la comunicazione e la notifica di eventuali violazioni di sicurezza, anche l'introduzione di un Registro dei trattamenti, della valutazione di impatto, della figura del Data Protection Officer (DPO), di nuovi concetti come ad esempio privacy by design e privacy by default, nonché della formazione riservata al personale [33].

Al fine di adeguarsi a questo nuovo sistema è di fondamentale importanza che le aziende non commettano alcuni errori: in particolare, esse devono intraprendere un percorso di adeguamento, mediante l'adozione di un approccio culturale e organizzativo, che è concepito solo per quanto riguarda il costo ma non deve essere considerato come un'opportunità per rafforzare la propria competitività.

Inoltre, le aziende non devono considerare tale sistema di protezione come uno strumento universale per risolvere tutti i problemi ma deve essere considerato come uno strumento che permette di adeguarsi alla normativa. L'approccio che viene implementato dalle aziende deve essere improntato a tre parole chiave; protezione, integrità e disponibilità dei dati personali, cosa che richiede al

[33] MACRI' E. e CASTIGLIA G., *Il nuovo regolamento europeo sulla privacy: un breve vademecum*, 2018.

personale aziendale di lavorare su tre fronti ovvero quello della governance, della law e della insurance che, ugualmente, si qualificano come pilastri delle organizzazioni aziendali [34].

Sulla base di queste indicazioni, le aziende sono state chiamate ad adeguarsi alla nuova normativa implementando tutte le misure necessarie per attivarla e per raggiungere gli obiettivi che prevede, predisponendo per l'organizzazione aziendale tutti i prodotti e i servizi conformi al gdpr [35].

Il primo passo che le aziende sono chiamate a compiere è quello di implementare un procedimento di valutazione dei dati che sia chiaro e attendibile e per farlo, nella maggior parte dei casi, esse scelgono di ricorrere a figure professionali qualificate che li aiutino a scegliere i metodi più attendibili per la gestione dei documenti e dei dati all'interno dell'azienda. L'aiuto di questa figura professionale è molto importante poiché, qualora l'azienda riscontri delle carenze, tale figura, essendo esperta e ben informata, consiglierà all'azienda stessa a quali strumenti hardware e software ricorrere affinché tutte le procedure e le misure utilizzate siano conformi alla normativa promulgata [36].

Un'importante risorsa, in questo caso, è rappresentata per le aziende dal ricorso ad un archivio centrale controllato e avente accesso limitato: esso permetterà di offrire un alto livello di sicurezza poiché l'accesso a questi dati sensibili sarà riservato solamente al personale autorizzato.

La previsione di nuove metodologie e nuovi strumenti per gestire i dati aiuterà, molto, le aziende anche a uniformare il processo di raccolta che riguardano non solo i dati ma tutti i documenti che fanno il loro ingresso in azienda: in questo modo si garantirà una gestione coerente dei dati personali che verranno classificati, indicizzati e archiviati mediante una metodologia che permetterà una facile e veloce consultazione e recupero [37].

Il GDPR, all'interno delle aziende, inoltre ha previsto due importanti garanzie: il diritto di accesso e il diritto all'oblio secondo i quali i soggetti interessati possono richiedere una copia di tutti i propri

[34] *Ibidem*.
[35] In realtà, pochissime organizzazioni sono in grado di fornire consulenza ad altre aziende, e le autorità stanno mettendo in guardia le persone affinché prestino la massima attenzione nel momento in cui decidono di affidare la sicurezza dei propri dati a imprese che sostengono di essere conformi al GDPR. Sebbene sia azzardato affermare che è possibile raggiungere la conformità seguendo procedure "preconfezionate", è anche vero che alcuni prodotti possono essere d'aiuto alle organizzazioni ai fini della conformità, per esempio la cifratura dei dati gestiti o l'automazione dei processi aziendali per il trattamento dei dati.
[36] Fra questi, per esempio, il miglioramento della sicurezza dei dati attraverso la crittografia end-to-end con il supporto del protocollo SSL e IPSec, l'utilizzo di sistemi di sovrascrittura dei dati e la protezione del disco rigido dei dispositivi di stampa. Un buon partner per il trattamento dei dati sarà anche in grado di gestire i dati originali richiesti o non richiesti provenienti dalle innumerevoli applicazioni back end e dai sistemi ERP aziendali.
[37] BIAISOTTI A., *Il nuovo regolamento europeo sulla protezione dei dati,* EPC editore, Roma.

dati personali come anche la cancellazione di tutti i dati vecchi che si rivelano essere non essenziali. Questo sistema di gestione dei dati renderà più semplice e più automatica anche l'implementazione del processo di cancellazione degli stessi nel momento in cui essi non serviranno più nonchè il processo di recupero qualora vi sia una richiesta del cliente [38].

3.2. Implicazioni per le imprese

Tra le novità apportate dal nuovo Regolamento sulla privacy le più importanti prevedono come destinatari proprio le imprese, onerate dall'obbligo di conformarsi in tempo alle nuove prescrizioni europee al fine di non imbattersi nelle relative sanzioni, nel caso in cui ci sia inosservanza in tal senso.

Se per le multinazionali e le aziende di maggiori che presentano maggiori dimensioni l'adeguamento al GDPR non ha implicato problemi di particolare rilievo, per gli enti pubblici e le piccole e medie imprese, viceversa, la situazione si è manifestata sin dall'inizio molto differente: l'assenza di attualità all'interno delle strutture organizzative e di avanzamento tecnologico degli strumenti impiegati ne hanno indubbiamente intralciato l'adeguamento, sebbene i termini imposti dal Regolamento fossero più che sufficienti per conseguire lo scopo atteso.

Tuttavia, le azioni riformatrici più importanti e gravose che incomberanno su tali soggetti sono circoscritte e possono essere compendiate in pochi punti.

In primo luogo, i soggetti che presentano i requisiti indicati dal Legislatore devono occuparsi della nomina di un *Data Protection Officer* (D.P.O.), ovvero un soggetto (che vedremo meglio spiegato nell'ultimo paragrafo) il quale presenta il precipuo compito di di occuparsi della gestione di tutte le pratiche concernenti il trattamento e la protezione dei dati personali.

Se l'attività di trattamento manifesta un pericolo elevato per i diritti e le libertà delle persone fisiche, in base all'art. 35 GDPR la società deve necessariamente rifarsi ai criteri di valutazione d'impatto sulla protezione dei dati (D.P.I.A., "*Data Protection Impact Assessment*"). Questo istituto definisce il trattamento dei dati personali e ne valuta la necessità e proporzionalità in rapporto agli interessi di impresa, mediante la valutazione del grado di rischio tollerabile.

L'impiego professionale dei dati personali è al momento anche dipendente alla conservazione di un registro per il trattamento: ai sensi dell'art. 30 GDPR, gravato di tale incombente è il Titolare (o se nominato il Responsabile) del trattamento, il quale deve provvedere a riportare all'interno del registro

[38] TOSHIBA – LEADING INNOVATION, *GDPR: cosa comporta per la vostra azienda*, in *Together information*, op. cit.

l'individuazione e la valutazione di tutti i trattamenti espletati, in modo tale da poterne regolarmente programmare e controllare il trend e la modalità di realizzazione.

Tali novità implicano poi la nascita di un aggiuntivo peso a carico delle imprese: nelle relazioni "esterne" con gli interessati occorrerà aggiornare e adeguare alla nuova regolamentazione la modulistica impiegata per il trattamento.

Infine, i destinatari del GDPR dovranno impiegare tutti gli strumenti appena presentati al fine di svolgere una globale valutazione di adeguatezza sui trattamenti dei dati personali che vengono attuati.[39]

3.3. Adeguamento delle imprese al GDPR: vantaggi e non

Il GDPR richiederà alle aziende di attuare una serie di trasformazioni rilevanti relativamente «*ai programmi di sicurezza, alle modalità di processare informazioni personali e alla gestione delle loro infrastrutture ICT*»[40] al fine di riuscire a garantire l'adeguata cura, preservazione, monitoraggio e protezione dei dati che hanno origine nell'Unione Europea, come anche la tutela del diritto alla privacy per ogni persona.

Il GDPR mira innanzitutto a consolidare la salvaguardia della privacy, a fornire a tutti i cittadini e a coloro che risiedono nel territorio europeo il controllo sui propri dati e a facilitare il quadro regolativo per gli enti che svolgono la loro funzione nell'UE.

La nuova normativa dovrà essere applicata a tutti gli enti che presiedono in UE e dispone regole puntuali per chiunque coordini, raccolga, custodisca, trasferisca o sparga dati sui cittadini europei.

Numerosi «*studiosi, avvocati specializzati, ed esperti di privacy*»[41] si domandano se il GDPR raffiguri in concreto una normativa valida ad individuare con facilità (e tutelare) ciò che rappresenta i dati personali di una persona, così come i titolari di imprese (in special modo se presentano piccole dimensioni) dovranno far fronte alle difficoltà e ai costi per il GDPR, scaturenti dal bisogno di allinearsi ai mutamenti organizzativi e procedurali richiesti dalla nuova normativa.

Ad esempio, gli obblighi di indicazione e notifica di attacchi cyber potrebbero comportare l'obbligo di inviare alla propria Autorità garante e altri eventuali referenti ("*points of contact*") per ogni Stato

[39] GDPR: cosa devono fare le aziende per adeguarsi, in https://www.gdpr.net/gdpr-cosa-devono-fare-le-aziende-per-adeguarsi/
[40] Impatto del GDPR sulle piccole e medie imprese: il buono, brutto e il cattivo, in https://www.agendadigitale.eu/sicurezza/impatto-del-gdpr-sulle-piccole-e-medie-imprese-il-buono-brutto-e-il-cattivo/
[41] Ibidem.

membro un numero estremamente elevato di informazioni[42] che potrebbero non essere gestite comodamente da una PMI che presenta indubbiamente risorse e capacità circoscritte rispetto ad un'azienda di maggiori dimensioni.[43]

Tra i vantaggi che le aziende ricevono dall'adeguamento al nuovo Regolamento possiamo elencare:

- Razionalizzazione dei processi e delle procedure: numerose PMI, nella ricerca affrettata dei benefici dal punto di vista competitivo che conduce verso una maggiore digitalizzazione, hanno attivato procedure, infrastrutture tecnologiche sempre più aperte e connesse, ma in maniera del tutto caotica e disomogenea, con la presenza di enormi vuoti nell'area della sicurezza. Per tale ragione si rivela necessario curare e ottimizzare «*l'aspetto dell'automazione dei dati, dei processi e della sicurezza nella sua globalità*»[44];
- Maggiore protezione dei dati che si pongono al centro di qualsiasi business: il GDPR nasce proprio prendendo in considerazione il panorama ormai incontenibile di cyber attacchi e minacce al capitale informatico e alla privacy di dirigenti e aziende. In un contesto che oramai si rivela ogni giorno essere sempre più connesso, sono proprio i dati ad essere il punto di partenza di ogni business, e come tale hanno bisogno di essere salvaguardati;
- Le aziende devono assicurare un determinato livello di sicurezza e dimostrare il regolare controllo della protezione dei dati. Devono essere capaci di creare prodotti o servizi che diano sicurezza al cliente nel momento in cui si accinge ad utilizzarli; ciò significa assicurare l'ottima riuscita del business.[45]

3.4. Scrivere un'informativa chiara e puntuale

L'informativa perde le sembianze di uno strumento fiscale e formalista. Deve essere resa in maniera breve, chiara, conoscibile e agevolmente accessibile, con l'impiego di un linguaggio agevole da capire, in particolar modo in tutte quelle ipotesi in cui le informazioni vengono indirizzate ai minori.

Pertanto, la finalità che vuole raggiungere il nuovo modello di informativa è quella di combattere il consenso fornito per pigrizia, mirando verso una concreta consapevolezza da parte dei soggetti, i quali

[42] Percepite in be 24 lingue.
[43] Impatto del GDPR sulle piccole e medie imprese: il buono, brutto e il cattivo, in https://www.agendadigitale.eu/sicurezza/impatto-del-gdpr-sulle-piccole-e-medie-imprese-il-buono-brutto-e-il-cattivo/
[44] GDPR: un'opportunità per le aziende, in https://www.neinformatica.it/it/gdpr-unopportunita-per-le-aziende-508.asp
[45] Ibidem.

devono essere adeguatamente informati anche relativamente alle tempistiche di mantenimento dei dati trattati.[46]

3.5. Il *Data Protection Impact Assessment* (DPIA)

La DPIA è uno strumento utile per la rilevazione circa la rischiosità o meno del trattamento. Si tratta di una procedura volta a rappresentare un trattamento dati e decretarne cosi necessità e adeguatezza oltre che i pericoli collegati. Tutto ciò ha il principale fine di affrontare i rischi stessi in maniera corretta. Non occorre che il DPIA si focalizzi su un singolo trattamento dal momento che questa procedura inerire trattamenti che manifestano similitudini e punti di contatto in materia di natura, pericoli, scopi e modalità.

Relativamente ai contenuti, l'art. 35 del *General Data Protection Regulation* riporta i seguenti elementi del DPIA:

- Una precisa descrizione dei trattamenti e delle corrispettive finalità oltre che, nel caso in cui sia possibile, il legittimo interesse del titolare;
- Prendendo in considerazione gli scopi che intende perseguire il trattamento, una valutazione circa la proporzionalità e le necessità;
- Una valutazione dei pericoli per i diritti e le libertà di ogni interessato;
- Prendendo in considerazione i diritti e gli interessi legittimi degli interessati, le misure disposte per far fronte ai pericoli comprendendo le essenziali garanzie di *data protection e compliance* GDPR.[47]

Il DPIA si rivela obbligatoria nelle seguenti ipotesi:

- Valutazione precisa e completa di aspetti personali inerenti alle persone fisiche, fondata sul trattamento automatizzato e profilazione sulla quale si basano determinate decisioni che possono racchiudere effetti legali o simili per le persone fisiche;
- Trattamento su vasta scala dei dati sensibili;
- Sorveglianza sistematica su vasta scala di una zona accessibile al pubblico.

Il DPIA, invece, non è obbligatorio:

[46] Normativa GDPR: cosa è e cosa cambia per le aziende, in https://www.raffaelegaito.com/gdpr-normativa-aziende/#Conoscere_il_proprio_business
[47] Swascan, Il GDPR per le piccole e medie imprese, Youcanprint, 2018.

- Per i trattamenti che non manifestano un alto pericolo per gli interessati;
- Se per un trattamento simile è già stato eseguito un DPIA;
- Nel caso in cui i trattamenti siano già stati assoggettati a controllo da parte dell'Autorità di controllo entro maggio del 2018 e le peculiarità del trattamento in questione non hanno subito modifica alcuna.

Il DPIA deve essere attuata prima che il trattamento venga posto in essere; è una valutazione preventiva assoggettata ad aggiornamenti periodici e costanti nel tempo.

La responsabilità del DPIA è del titolare del trattamento, mentre la sua attuazione pratica può essere espletata da qualcun altro. Il titolare, in ogni caso, ha l'obbligo di controllare il processo rivolgendosi regolarmente al DPO.[48]

3.6. Nominare il *Data Privacy Officer* (DPO)

Il *Data Protection Officer* è una figura inserita dal Regolamento generale sulla protezione dei dati 2016/679 GDPR, pubblicato sulla GU europea L. 119 il 4 maggio 2016.

Il DPO, figura nei fatti già presente in varie legislazioni europee, è un esperto che deve svolgere un ruolo aziendale (sia che si tratti di un soggetto interno o esterno) con abilità giuridiche, informatiche, di *risk management* e di analisi dei processi.

La sua principale responsabilità è quella di esaminare, determinare e organizzare la gestione del trattamento di dati personali (e dunque la loro relativa protezione) in un'azienda (sia che si tratti di un'azienda pubblica che privata), affinché questi siano trattati nel rispetto delle norme sulla privacy.

Questo soggetto è noto nell'universo anglosassone con la locuzione di *Chief Privacy Officer* (CPO) *Privacy Officer*, *Data Protection Officer* o *Data Security Officer*.[49]

3.7. I costi richiesti alle aziende

L'adeguamento richiesto alle aziende alla nuova normativa del GDPR richiederà una spesa significativa e, spesso, molte aziende devono fare i conti con un budget disponibile limitato. Sicuramente, non è possibile definire, in questa sede, delle quantificazioni assolute della spesa a cui le aziende andranno incontro ma è possibile fare delle riflessioni.

[48] Ibidem.
[49] Chi è il Data Protection Officer?, in https://www.assodpo.it/it/chi-e-il-dpo/

Da una ricerca effettuata dalla International Association of Privacy Professional è emerso, dall'analisi di un campione di 600 esperti di privacy di tutto il mondo, che 75% delle multinazionali europee ovvero quelle società che possiedono più di 75.000 dipendenti, devono riservare al processo di adeguamento al GDPR un investimento di almeno 5 milioni di euro, a cui farà seguito anche l'assunzione di due o tre figure professionali che saranno impegnate costantemente nell'ambito della privacy. La ricerca ha, inoltre, rilevato che la stessa tipologia di investimenti saranno effettuati anche dal 50% delle grandi multinazionali negli Stati Uniti d'America. I 600 esperti che sono stati interpellati all'interno di questa ricerca hanno rilevato che delle 30.000 aziende con le quali si sono interfacciati solo il 60% sarà in grado di adeguarsi conformemente alla normativa entro la fine del 2018 poiché molte aziende non sono riuscite a rispettare la scadenza prevista dalla normativa europea per quanto riguarda l'adeguamento normative [50].

Se prendiamo in analisi, invece, le aziende di dimensioni più ridotte, che non siano le grandi multinazionali, il valore medio a cui ammonta l'investimento per adeguarsi alla normativa del GDPR nel 2016 era di 349.000 euro mentre nel 2017 è salito a 480.000 euro: la levitazione di questi costi è stata determinata dal nuovo ruolo riservato al DPO, dai costi riservati ai consulenti e dagli investimenti effettuati nell'ambito dell'Information Technology per adeguarsi a quanto stabilito dal Regolamento [51].

Queste cifre consacrano il GDPR come un significativo investimento per le aziende e, allo stesso tempo, come un'opportunità per gli esperti in materia. In effetti, questi ultimi, poiché la normativa stabiliva due anni di tempo per dare la possibilità alle aziende di adeguarsi, hanno scelto di sfruttare questo arco di tempo per affinare le proprie competenze nell'ambito della GDPR.

Se ci concentriamo sulla situazione italiana, invece, nel nostro tessuto economico non sono presenti quelle grandi multinazionali che hanno scelto di investire 5 milioni di euro per adeguarsi al GDPR poiché le piccole e medie imprese hanno capacità di investimento ridotti e sulla base del budget limitato devono plasmare le proprie scelte strategiche per quanto riguarda il processo di adeguamento del GDPR. Alcune aziende preferiscono imboccare la strada dell'adeguamento più informale che sostanziale della normativa mediante la revisione delle informative, la regolamentazione e il trasferimento dei dati all'estero, le nuove politiche nei confronti dei dipendenti, mentre altre effettuano più una scelta mirante a revisionare il parterre dell'Information Technology che spesso si rivela essere profondamente inadeguato alla normativa attuale. Il risultato di questo panorama che si è definito in

[50] *GDPR, quanto costerà a una pmi adeguarsi (e come ottimizzare la spesa)*, 2017, Fonte: www.agendadigitale.eu
[51] L'investimento complessivo nel 2017 è stato di 6,5 Miliardi di Euro su 30.000 aziende.

Italia permette di tirare delle somme: il 78% delle aziende italiane ancora non è pronto ad adeguarsi alla normativa del GDPR a causa del limitato budget messo a disposizione. Tuttavia, affinché le aziende italiane riescano ad adeguarsi usufruendo del budget limitato potrebbero dotarsi di personale specializzato che aiuti l'azienda ad assorbire quel cambio di paradigma nella gestione dei dati nell'ottica di un nuovo principio di accountability. Questo incarico, solitamente, non deve essere assegnato solo ad un professionista nell'area legale ma anche ad un professionista informatico: la soluzione ideale sarebbe di scegliere una persona che possegga entrambe le caratteristiche. Inoltre, per poter incrementare la fase di adeguamento le aziende italiane sono chiamate a nominare un DPO, meglio se assunto al di fuori dell'azienda a meno che non sia presente, all'interno di essa, un soggetto che possieda tale competenza specifica in materia. Questa nuova figura rappresenta un punto di riferimento per tutti i soggetti e dipendenti che stanno lavorando per adeguare l'azienda alla nuova normativa.

Infine, anche l'investimento nell'Information Technology rappresenta un passo molto importante per adeguare l'organizzazione aziendale alla normativa, avvicinandosi sempre di più anche a degli standard riconosciuti a livello internazionale. In effetti, adottare tale normativa non vuol dire solamente assorbire una metodologia di gestione che permetterà di gestire in maniera legale i dati personali di terzi o di propri dipendenti, ma permetterà anche di predisporre un sistema di protezione del proprio know-how aziendale che oggi è sempre di più messo in pericolo dalle attività illegali che vengono poste in essere da cybercriminali o da dipendenti infedeli. L'adeguamento alla normativa si qualifica come una scelta obbligata anche perché imposta dal legislatore e, come abbiamo visto, richiede un'ingente spesa ma, è stato rilevato, che anche il mancato adeguamento alla normativa può determinare dei costi non indifferenti per l'azienda. In effetti, nel caso in cui venga riscontrata una violazione nel trattamento e nella protezione dei dati personali la sanzione verrà quantificata secondo una stima che oscilla tra i 20 milioni di euro e il 4% del fatturato; ad esempio, per un'azienda che ha 5 milioni di fatturato il 4% ammonta a 200 mila euro: una violazione richiederebbe il pagamento di tale somma. Proprio per evitare di incorrere in spese inutili e per adeguarsi alla normativa è necessario che le aziende investino su queste iniziative perché investire su di esse vuol dire anche investire sul futuro e nessuna azienda, neanche quella che sia la più "offline", potrà sottrarsi dall'implementazione di tale trattamento che regalerà al dato personale maggiore protezione e sicurezza. Inoltre, il mancato adeguamento può far sorgere maggiori preoccupazioni, sia da parte delle aziende che da parte della clientela, per via del rischio che vi possa essere una violazione dei dati personali da parte di hackers, un errato utilizzo della privacy da parte dei dipendenti che non possiedono le adeguate competenze in questo ambito o una mancata compliance dell'azienda. I risvolti negativi non riguardano solamente

la sanzione ma riguardano anche l'immagine e la reputazione dell'azienda perché, sicuramente, nessun cliente vorrà comunicare i dati della propria carta di credito ad un'azienda che si rivela essere inefficace nella protezione dei dati personali dei suoi clienti. Pertanto, si può affermare con chiarezza che l'inosservanza delle disposizioni contenute nel Regolamento e il mancato adeguamento normativo ad esso può apportare seri danni all'immagine aziendale, determinando delle conseguenze negative nelle vendite, nel marketing e nelle relazioni con i clienti e gli stakeholder.

3.8. Nuovo Regolamento e call center

Aziende di call center e associazioni dei consumatori mettono insieme le loro forze contro il telemarketing selvaggio.

Peculiare attenzione è rivolta al trattamento dei dati personali dei clienti e all'allineamento rispetto a quanto stabilito dal GDPR.

Le imprese che eseguono attività di telemarketing e che gestiscono dati personali di clienti /consumatori, se disposto dalla legge, debbono provvedere alla nomina di un DPO, così come avvalorato dal Garante per la Protezione dei Dati Personali.[52]

Relativamente ai call center, le attività di telemarketing e teleselling, il nuovo Regolamento permette:

- Di registrare il proprio numero di cellulare e fisso al registro delle opposizioni, anche se non risultano iscritti negli elenchi telefonici; in poche parole, ogni utenza al momento presente potrà fare l'iscrizione;
- La revoca di tutti i consensi al trattamento dei dati personali espressi in un momento antecedente;
- La proibizione di cessione di elenchi telefonici a terzi;

I call center devono:

- Immettere un numero riconoscibile e ricontattabile in maniera tale che, anche se non si vuole provvedere all'iscrizione nel registro sopracitato, coloro che ricevono le chiamate possono avvalersi del diritto di recesso contattando nuovamente il numero che li ha contattati;

[52] Sfida GDPR per i call center: ecco il nuovo Codice etico, in https://www.corrierecomunicazioni.it/telco/sfida-gdpr-per-i-call-center-ecco-il-nuovo-codice-etico/

- Impiegare un prefisso, nel caso in cui non vengano utilizzati numeri ricontattabili, in maniera che coloro che hanno deciso di non effettuare l'iscrizione nel registro se ricevono la chiamata possono subito riconoscere che si tratta di una chiamata commerciale.[53]

Le aziende che lavorano nell'ambito di questo settore devono regolarmente controllare le condizioni dirette ad assicurare un'esatta efficienza dei call center, sia se sono programmati nell'articolazione dell'Operatore stesso, sia nel caso in cui l'attività è contrassegnata dalla sussistenza di una Impresa committente che appalta ad una differente azienda di servizi l'attività dei call center (spesso trasferiti all'estero).[54]

[53] GDPR: cosa cambia per i software crm e i call center?, in https://www.crm4solution.com/gdpr-cosa-cambia-software-crm-call-center/
[54] Call Center e il rispetto delle regole sulla privacy, in https://legaldesk.it/blog/call-center-privacy

4. Le sanzioni

Con l'entrata in vigore del GDPR, la cornice sanzionatoria sarà certamente più rigida, non solamente per ciò che concerne la natura degli importi, ma anche relativamente ai casi per cui possono essere comminate le sanzioni.

Prima di analizzare maggiormente nel particolare il meccanismo del quadro regolatorio, occorre sottolineare la scelta adottata dal legislatore europeo di unificare e standardizzare la tipologia e l'entità delle sanzioni, diversamente da quanto avveniva in passato, dando *ex ante* alcuni criteri per l'analisi delle sanzioni amministrative pecuniarie.

Il Working Party Articolo 29 ha così reputato indispensabile emanare delle linee guida, affinché venisse assicurata, da una parte, l'applicazione coerente delle regole sulla tutela dei dati personali, dall'altra, un regime di tutela dei dati equilibrato per tutti i cittadini europei.

Sulla scorta dell'art. 82 del GDPR, viene salvata la possibilità per l'interessato, che patisca un pregiudizio materiale o immateriale, di conseguire il risarcimento del pregiudizio subito, a seconda che la trasgressione sia stata posta in essere dal Titolare o dal Responsabile.

Relativamente alle sanzioni amministrative pecuniarie e/o penali, il GDPR, regolamenta le situazioni per cui viene disposta l'applicazione di sanzioni amministrative pecuniarie e/o penali. Per ciò che concerne le prime esse possono arrivare a 10 milioni di euro o, se superiore, il 2% del fatturato mondiale nei casi di (a titolo dimostrativo):

- inosservanza delle condizioni che devono essere applicate al consenso dei minorenni in rapporto ai servizi della società dell'informazione;
- trattamento proibito di dati personali che non abbisogna dell'individuazione dell'interessato;
- fallita o erronea notificazione di un *data breach* all'Autorità nazionale competente;
- inosservanza dell'obbligo di nominare il DPO;
- mancata applicazione di misure di sicurezza.

L'importo delle sanzioni amministrative pecuniarie può giungere sino a 20 milioni di euro ovvero al 4% del fatturato mondiale dell'azienda nelle ipotesi di (a titolo dimostrativo):

- trasgressione di un ordine, di un freno temporaneo o definitivo inerente a un trattamento, imposti da un'Autorità nazionale competente;

- trasferimento vietato *cross-border* di dati personali ad un destinatario in un Paese terzo.

Di seguito i criteri che vengono adottati per la determinazione delle sanzioni amministrative pecuniarie che troviamo elencate all'art. 82, par. 2:

- la natura, l'importanza e la durata dell'inosservanza attuata;
- il carattere doloso o colposo caratterizzante l'inosservanza;
- il livello di collaborazione con l'autorità di controllo in maniera da rimediare all'inosservanza e attutirne le probabili conseguenze negative[55].

Per ciò che concerne il primo criterio, il Regolamento riconosce la presenza di svariati massimali per le sanzioni amministrative pecuniarie, i.e. 10 o 20 milioni di euro.

Sarà, pertanto, onere dell'Autorità nazionale competente valutare le circostanze del caso, sulla base di tali criteri generali, e poi capire se procedere o meno con una misura correttiva sotto forma di sanzione pecuniaria.

Nel Considerando 148, viene data all'Autorità nazionale la possibilità di rimpiazzare la sanzione pecuniaria con un ammonimento, "*in caso di violazione minore o se la sanzione pecuniaria che dovrebbe essere imposta costituisse un onere sproporzionato per una persona fisica*".

Anche questo inciso prova l'attitudine del legislatore europeo di favorire l'impiego delle sanzioni pecuniarie con un approccio "ponderato" ed "equilibrato". Il fine ultimo resta, in ogni caso, quello di incoraggiare le imprese al rispetto della privacy, affidando lo strumento dell'applicazione di sanzioni pecuniarie così alte, unicamente, al fine di contrastare in modo persuasivo e proporzionato ad eventuali trasgressioni.

Per quanto riguarda il secondo criterio, le valutazioni, inerenti alla sussistenza di dolo o di colpa nella condotta, dovranno essere realizzate sulla scorta di elementi oggettivi e sarà ruolo della giurisprudenza emergente definire *ex ante* "*linee di demarcazione più chiare per valutare il carattere doloso di una violazione*". Il *Working Party* ha, tuttavia, già facilitato alcune condotte che potranno integrare il suddetto carattere doloso. Queste sono riconducibili alle ipotesi di:

- trattamenti proibiti accordati espressamente dal *senior management* o non dando importanza ai pareri formulati dal DPO;

[55] GDPR: le sanzioni, in http://www.altalex.com/documents/news/2018/04/04/gdpr-le-sanzioni-privacy

- cambiamento di dati personali, avente lo scopo di dare un'impressione "fuorviante" circa il raggiungimento degli obiettivi precisati;
- vendita di dati, in assenza di controllo e/o tralasciando la scelta liberamente espletata dagli interessati.

Relativamente al terzo criterio, ciò che va evidenziato sarà il grado e la natura della collaborazione con le autorità di controllo. Esso potrà raffigurare un elemento decisivo, nella scelta di adottare o meno una sanzione amministrativa e, eventualmente, disporne il totale, nel caso in cui siano state circoscritti o annullati i contraccolpi negativi sui diritti degli interessati che si sarebbero altrimenti concretizzati in assenza di tale cooperazione.[56]

[56] Ibidem.

5. Case study: Canon

5.1. Canon: azienda leader che si adegua al GDPR

Il Regolamento europeo relativo alla protezione dei dati personali ha determinato delle conseguenze notevoli sulle organizzazioni aziendali poiché ha influenzato, profondamente, lo svolgimento di molte attività da quelle relative alla gestione del cliente fino a quelle relative alla gestione interna. Per poter rimanere sempre al passo con i tempi e con la normativa le aziende sono chiamate ad implementare delle solide politiche per disciplinare, in maniera legale, il processo di gestione delle informazioni e dei documenti.

Tra le varie aziende che hanno dovuto adeguarsi alla nuova normativa vi è anche la multinazionale Canon il cui Directory Information Management Solutions and Services, Giuseppe D'Amelio, ha affermato che l'applicazione del GDPR in azienda ha richiesto un rinnovamento dei processi nell'ottica di implementazione di una trasformazione digitale riguardante i dati personali [57].

Egli, infatti, ha sostenuto che la modifica dei processi e dei modelli relativi alla gestione documentale è stata determinata dall'incremento dell'intelligenza artificiale in azienda, dal processo di trasformazione digitale che è stato avviato da qualche anno, dall'analisi dei dati e dall'aumento dei contenuti come immagini e video che hanno cominciato a veicolare all'interno dell'organizzazione aziendale. Tutti questi elementi hanno determinato un maggiore livello di complessità nella gestione documentale.

Uno dei fattori molto importanti per l'azienda Canon che è stato introdotto dalla nuova normativa è proprio la classificazione delle informazioni: in effetti l'azienda, come ha affermato D'Amelio, se inizialmente classificava le informazioni all'interno di uno specifico registro dei dati, adesso con la promulgazione del GDPR il dato personale, essendo correlato ad altre informazioni, viene concepito sotto una nuova veste, ovvero come dato sensibile e così lo stesso Regolamento assicura, mediante le proprie disposizioni, la tutela del dato personale inteso come diritto fondamentale del cittadino [58].

[57] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.
[58] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.

5.2. La sicurezza informatica

L'introduzione del GDPR, quindi, anche all'interno dell'azienda Canon ha introdotto un preciso processo di gestione documentale il cui svolgimento non è riservato esclusivamente al responsabile ma a tutte le risorse dell'azienda che devono collaborare per dare applicazione a quanto stabilito dalla normativa. All'interno della canon, come in molte altre aziende, la tutela dei dati personali è strettamente correlata alla sicurezza che non riguarda solamente una questione tecnologica o innovativa, come ha sottolineato D'Amelio, ma riguarda un problema culturale poiché eventuali comportamenti incauti e superficiali possono essere fortemente dannosi per le aziende e proprio per evitare inconvenienti del genere la classificazione delle informazioni si qualifica come un processo molto importante [59]. Canon, adeguandosi alla normativa, ha implementato delle soluzioni in grado di conservare il dato personale, che ha avuto accesso nel sistema, solo per il tempo necessario per raggiungere l'obiettivo per il quale è stato raccolto.

Allo stesso modo, l'azienda mette in atto delle procedure per distruggere il dato in maniera sicura nel momento in cui è diventato obsoleto, ottimizzando gli spazi fisici e digitali, abbassando i costi di conservazione e preservando tutta la documentazione che, tuttavia, potrebbe ritornare utile qualora si verificasse un contenzioso. In particolare, il contributo di Canon mira anche ad aiutare tutte le altre aziende a proteggere e gestire i dati a fronte di un eventuale comportamento incauto. Uno degli strumenti che è stato implementato è la piattaforma "Therefore" che prevede una precisa gestione documentale: questo processore permette di archiviare, cercare e catalogare tutti i dati personali nel rispetto di ogni standard di sicurezza [60].

Questa piattaforma è stata introdotta sul mercato ed è a disposizione anche di tutte le altre aziende, qualora, volessero acquistarla ma a differenza di tutte le altre piattaforme presenti sul mercato questa è in grado di gestire sia i dati personali sia quelli che sono già stati inseriti nel database, ricomprese anche le immagini e i video. La piattaforma, inoltre, può essere attivata mediante il ricorso al classico meccanismo on premise, ma anche in cloud. Canon, inoltre, ha predisposto anche un servizio di formazione per le aziende e per i professionisti al fine di far emergere delle competenze specifiche per assicurare una gestione documentale di qualità, capace di rispettare quanto stabilito dalla normativa [61].

[59] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.
[60] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.
[61] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.

5.3. Analizzare i contenuti dei documenti

Canon, inoltre, dispone di un personale molto qualificato in azienda nell'ambito della gestione informatica ma nonostante questa preparazione professionale spesso risulta molto difficile l'analisi dei contenuti soprattutto per quanto riguarda la gestione dei documenti. Canon, poiché rimane sempre al passo con i tempi, ha implementato "Uniflow" la soluzione per ottimizzare la stampa e la scansione al fine di dare la possibilità ai dipendenti e agli utenti di stampare dai loro dispositivi mobili.

Questo meccanismo garantisce tutti i meccanismi di stampa in sicurezza mediante l'ausilio di badge o impronte digitali. La piattaforma, allo stesso tempo, analizza tutti i documenti sia in entrata che in uscita mediante l'attivazione di un alert che si attiva se vengono rilevate specifiche parole chiave o altre condizioni stabilite dall'utente. Inoltre Canon, al fine di rispondere alle esigenze dei clienti, per quanto riguarda l'applicazione della normativa, ha predisposto un'ampia gamma di servizi mediante l'acquisizione di Integra Document Management che si qualifica come parte fondamentale del Business Information Service di Canon, specializzata in servizi di Document e Business Process Outsourcing [62].

Canon, infatti, si qualifica come un'azienda leader in Italia per la gestione in Outsourcing di processi documentali per le compagnie assicurative, per i gruppi bancari e finanziari e tra i propri clienti conta alcune società leader nei settori Telco, Media, Retail e GDO.

5.4. Le fasi di gestione delle informazioni

L'azienda, inoltre, ha attivato un approccio alla governance delle informazioni in modo circolare mediante la previsione di alcune importanti fasi:

- la prima fase è la c.d. discover che permette di individuare i dati raccolti e prevede specifiche modalità di conservazione, dopo l'analisi dei rischi riscontrati in questo step;
- la seconda fase è la c.d. secure che richiede la definizione di corrette politiche di sicurezza nonchè l'implementazione di strumenti e processi correlati;
- la terza fase e il c.d. menage all'interno della quale viene tracciato l'accesso dei dati creando workflow automatizzati e sicuri;

[62] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.

- la quarta e ultima fase è la fase di report che riguarda tutte le operazioni che sono tracciate in modo da poter revisionare, periodicamente, le policy e i processi attivati [63].

La normativa del GDPR, al contrario di quanto affermano tutti, non prevede dei criteri stringenti poiché i dati possono essere conservati per il tempo necessario anche se non stabilisce per quanto tempo. In questo ambito concede una certa libertà alle aziende anche se questa libertà può essere considerata come un'arma a doppio taglio capace di creare delle problematiche per l'azienda. In effetti, questo presupposto impone che il titolare della gestione dei dati personali abbia una maggiore conoscenza e che sia consapevole sia del tipo di documento che ha fatto accesso in azienda sia delle informazioni che contiene al fine di implementare una gestione corretta di suddetti dati. La differenza la fa proprio la scelta del partner per assicurare la gestione documentale. Come ha osservato D'Amelio, alcuni importanti strumenti previsti dalla normativa come il massimario di conservazione e scarto e il registro del trattamento dei dati devono essere assorbiti dai processi aziendali e per poter introdurre questi strumenti è necessario avere partner competenti, senza determinare un appesantimento dei processi.

Affinché tutto avvenga nel migliore dei modi è necessario promuovere una stretta collaborazione tra le figure impiegate al fine di monitorare, salvaguardare e rendere disponibili i dati in outsourcing. Canon si qualifica come un'azienda in grado di offrire questo servizio e per i propri clienti conosce bene i processi aziendali che li riguardano e come integrare questi nuovi strumenti al sistema informativo dell'azienda [64]. La normativa, come ha affermato D'Amelio, favorisce lo sviluppo tecnologico e lo sviluppo economico, estendendo la tutela dei dati personali come un diritto fondamentale riservato a tutti gli utenti. Tuttavia, come spesso accade, la tecnologia tende a fare passi più lunghi rispetto alla normativa e per questo motivo è di fondamentale importanza che le aziende si dotino di personale e partner specializzato capaci di saper cogliere le opportunità offerte l'innovazione tecnologica rimanendo sempre entro il quadro tracciato dalla normativa [65].

[63] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.
[64] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.
[65] *Gli effetti del GDPR sulle PMI. Il caso Canon*, 2018, fonte: www.fabbricafuturo.it.

6. Conclusione

Secondo quanto emerge dal presente lavoro di tesi il Regolamento n. 679 del 2016, che ha dato attuazione al GDPR, è nato per raggiungere obiettivi di garanzia giuridica, di semplificazione amministrativa e di tutela nel trattamento e nel trasferimento di dati personali sia all'interno del territorio europeo che al di fuori dei confini comunitari.

Ad oggi, il Regolamento [66] si qualifica come una risposta necessaria per far fronte alle sfide future che sono poste davanti alle aziende dall'innovazione tecnologica poiché un trattamento dei dati efficiente si qualifica come tassello fondamentale per garanzia di crescita economica delle aziende. Il Regolamento, infatti, introduce delle disposizioni più chiare per quanto riguarda il trattamento dei dati personali ad opera delle figure responsabili, definendo anche i limiti che le aziende si pongono per assicurare tale trattamento. La normativa, infatti, stabilisce dei criteri rigorosi che devono essere rispettati per il trasferimento dei dati al di fuori dell'Unione Europea nonché delle specifiche sanzioni qualora si verificasse la violazione della normativa.

In sostanza, il GDPR rappresenta un valido strumento per il futuro delle aziende poiché consentirà sia quest'ultime che agli utenti a cui si rivolgono di poter esercitare questi nuovi diritti che sorgono bisognosi di tutela. Le aziende, da questo momento in poi, sono chiamate a rispettare queste nuove regole e qualora vadano incontro a comportamenti insolventi rischieranno sanzioni molto pesanti. Le priorità operative che la normativa richiede di implementare alle aziende nell'immediato futuro sono:

- la nomina del Responsabile della protezione dei dati personali (DPO);
- l'istituzione del Registro delle attività di trattamento;
- la notifica della violazione dei dati, il c.d. data breach.

L'attuale sviluppo tecnologico, al punto in cui è arrivato oggi, considera i dati, addirittura, come una sorta di merce di scambio cosa che ha concepito la privacy come un diritto che spesso risulta essere difficile da tutelare. In quest'ottica, la protezione dei dati personali e gli obblighi che da essi derivano non devono essere considerati come semplice adempimenti burocratici poiché l'adeguamento delle aziende a questa normativa si qualifica come un investimento fondamentale per il futuro al fine di poter far fronte alle sfide del mercato e proiettarsi nel futuro. È ormai chiaro a tutti che ogni attività

[66] Si tratta quindi di regole che, se da un lato comportano senz'altro uno sforzo per assicurare la totale conformità del proprio modello di business e delle sue implicazioni pratiche, dall'altro rappresentano certamente un importante incentivo e un valore aggiunto per le aziende che dimostrano di "essere in regola".

produttiva e aziendale prevede fattori come data analysis, big data, intelligenza artificiale e così via e internet stesso rappresenta il futuro delle aziende: proprio in un contesto fortemente volubile come può essere quello della rete garantire la qualità del trattamento dei dati, verificarne l'origine e controllare che il loro utilizzo avvenga secondo la normativa rappresenta un tassello fondamentale per la sopravvivenza delle aziende in future.

Per questo, le disposizioni del GDPR rappresentano il vero futuro dell'azienda poiché quanto in esse contenuto, se attuato adeguatamente, rappresenta il migliore investimento che le imprese possono attuare.

Le aziende, inoltre, sono chiamate ad investire nell'acquisto di software di qualità in grado di gestire tutti gli aspetti che emergono a fronte di un eventuale rischio privacy e che sia dotato di un'interfaccia di facile utilizzo che consenta la condivisione e il trattamento del dato: questo meccanismo permetterà di realizzare un sistema documentale integrato che sarà in grado di effettuare una comunicazione automatica ed attivare il meccanismo di alerting qualora ce ne fosse motive, assicurando alti livelli di reportistica.

Pertanto, secondo quanto emerge dal presente lavoro di tesi la sicurezza dei dati e il diritto attribuito agli utenti di controllare l'utilizzo che si fa dei propri dati personali si qualificano come materie fondamentale tanto in ambito nazionale quanto in ambito comunitario. La stessa Unione Europea, avendo preso consapevolezza delle ripetute violazioni di dati che si sono verificate nel corso degli anni e che hanno riguardato tanto il territorio comunitario quanto il territorio extracomunitario, ha compreso che era necessario rivedere la normativa, ovvero quella che risaliva al 1995, e promulgare un nuovo impianto normativo capace di assicurare una migliore gestione dei dati personali tanto nelle piccole e medie imprese quanto nelle grandi multinazionali [67].

Il GDPR viene, in questo modo, impostato al fine di elevare gli standard di qualità nella tutela nel trattamento del dato personale, spingendo le stesse aziende a migliorare i processi e a designare delle figure aventi il compito di controllare che tutto proceda secondo la normativa.

[67] Soprattutto quando si parla di nuove imprese innovative, il GDPR favorisce la creazione di un rapporto di fiducia tra realtà tecnologiche e imprenditoriali e consumatori. L'introduzione di regole nuove e decisamente più restrittive delle precedenti implica l'attribuzione di ruolo di "custode" a quelle realtà che si occupano di raccolta dei dati relativi agli utenti, arricchendo così un rapporto che prima veniva creato sulla base del mero interesse economico e allontanando l'aura di sospetto e ambiguità che troppo spesso caratterizza le relazioni Business to Consumer.

7. Referenze

7.1. Bibliografia

BASSOLI E., *La nuova privacy GDPR dopo il D. lgs. 10 agosto 2018, n.101. Guida teorico-pratica con schemi riassuntivi e formulario dei principali adempimenti*, Dike Giuridica, Milano, 2018.

CUCUMILE P., *Sulla tutela dei dati personali delle persone fisiche. Il contenuto del nuovo G.D.P.R.*, Franco Angeli, Milano, 2017.

DE STEFANI F., *Le regole della privacy. Guida pratica al nuovo GDPR*, Hoepli, Milano, 2018.

FUMAGALLI MERAVIGLIA M., *Le nuove normative europee sulla protezione dei dati personali* in *Diritto comunitario e degli scambi internazionali*, 2016.

IASELLI M., *Le nuove disposizioni nazionali sulla protezione dei dati personali. Il D.Lgs. n. 101/2018 di adeguamento al GDPR*, EPC, Milano, 2018.

MARINI P., *GDPR: il nuovo regolamento europeo sulla privacy*, Wolters Kluwer Italia, Milano, 2018.

NUCCI G., *Protezione dei dati personali e GDPR: dai precetti giuridici ai processi organizzativi*, Ipsoa, Milano, 2018.

RICCIO G. M., SCORZA G. e BELISARIO E., *GDPR e normativa privacy. Commentario*, Ipsoa, Milano, 2018.

RUGANI G., *Il Nuovo Pacchetto europeo sulla protezione dei dati personali: dalle origini al diritto all'oblio*, Università degli studi di Pisa, Pisa, 2017.

BIAISOTTI A., *Il nuovo regolamento europeo sulla protezione dei dati,* EPC editore, Roma.

MACRI' E. e CASTIGLIA G., *Il nuovo regolamento europeo sulla privacy: un breve vademecum*, 2018.

AMATO, F., SBARAGLIA, G., (2018). *GDPR. Kit di sopravvivenza. Capirlo, applicarlo ed evitare sanzioni sulla privacy e il trattamento dei dati personali*. Firenze: goWare.

DE STEFANI, F., (2018). *Guida pratica al nuovo GDPR*. Milano: Hoepli.

7.2. Sitografia

Toshiba – leading innovation, *gdpr: cosa comporta per la vostra azienda*, in *Together information*, 2016, disponibile da: www.toshibatec.it

GDPR: Quali opportunità per le aziende?, Circolare 3/2018, disponibile da: www.morganemorgan.it

GDPR, quanto costerà a una pmi adeguarsi (e come ottimizzare la spesa), 2017, disponibile da: www.agendadigitale.eu

Gli effetti del GDPR sulle PMI. Il caso Canon, 2018, disponibile da: www.fabbricafuturo.it.

Redazione Altalex, (2018). *Art. 5 GDPR - Principi applicabili al trattamento di dati personali*. Disponibile da http://www.altalex.com/documents/news/2018/04/12/articolo-5-gdpr-principi-trattamento-di-dati-personali

Legaldesk, (2018). *Call Center e il rispetto delle regole sulla privacy*. Disponibile da https://legaldesk.it/blog/call-center-privacy

Asso DPO, (n.d.). *Chi è il Data Protection Officer?*. Disponibile da https://www.assodpo.it/it/chi-e-il-dpo/

Samarati M., (2018). *GDPR: ambito di applicazione materiale e territoriale*. Disponibile da https://www.itgovernance.eu/blog/it/gdpr-ambito-di-applicazione-materiale-e-territoriale

Crm4Solution, (n.d.). *GDPR: cosa cambia per i software crm e i call center?*. Disponibile da https://www.crm4solution.com/gdpr-cosa-cambia-software-crm-call-center/

GDPR, (n.d.). *GDPR: cosa devono fare le aziende per adeguarsi.* Disponibile da https://www.gdpr.net/gdpr-cosa-devono-fare-le-aziende-per-adeguarsi/

Diritti e Risposte, (n.d.). *GDPR: i diritti degli interessati, diritti e risposte per comprendere e risolvere*. Disponibile da http://www.dirittierisposte.it/Schede/Tutela-della-privacy/Diritti/gdpr_i_diritti_degli_interessati_id1173414_art.aspx#Diritto%20di%20cancellazione%20o%20diritto%20all%C2%BFoblio%20(art.17)

Redazione Altalex, (2018). *GDPR: le sanzioni*. Disponibile da http://www.altalex.com/documents/news/2018/04/04/gdpr-le-sanzioni-privacy